

Titre: Défaillances au sein de réseaux interdépendants : les défis de la
Title: mise en place d'un système d'alerte précoce

Auteur: Cédric Debernard
Author:

Date: 2011

Type: Mémoire ou thèse / Dissertation or Thesis

Référence: Debernard, C. (2011). Défaillances au sein de réseaux interdépendants : les défis
Citation: de la mise en place d'un système d'alerte précoce [Mémoire de maîtrise, École
Polytechnique de Montréal]. PolyPublie. <https://publications.polymtl.ca/587/>

 **Document en libre accès dans PolyPublie**
Open Access document in PolyPublie

URL de PolyPublie: <https://publications.polymtl.ca/587/>
PolyPublie URL:

**Directeurs de
recherche:** Benoît Robert
Advisors:

Programme: Maîtrise en génie industriel
Program:

UNIVERSITÉ DE MONTRÉAL

DÉFAILLANCES AU SEIN DE RÉSEAUX INTERDÉPENDANTS : LES DÉFIS
DE LA MISE EN PLACE D'UN SYSTÈME D'ALERTE PRÉCOCE

CÉDRIC DEBERNARD

DÉPARTEMENT DE MATHÉMATIQUES ET GÉNIE INDUSTRIEL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INDUSTRIEL)

JUIN 2011

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

DÉFAILLANCES AU SEIN DE RÉSEAUX INTERDÉPENDANTS : LES DÉFIS
DE LA MISE EN PLACE D'UN SYSTÈME D'ALERTE PRÉCOCE

Présenté par : DEBERNARD Cédric

en vue de l'obtention du diplôme de : MAÎTRISE ÈS SCIENCES APPLIQUÉES

a été dûment accepté par le jury d'examen constitué de :

M. BOURGAULT Mario, ing., Ph.D., président

M. ROBERT, Benoît, ing., Ph.D., membre et directeur de recherche

M. SABOURIN, Jean-Pierre, M.A, membre externe

REMERCIEMENTS

Conclure dix-huit mois de recherche par une maîtrise en sciences appliquées au sein d'une école d'ingénieur au Québec lorsque l'on n'est soi-même ni ingénieur ni québécois ne peut se concevoir sans un certain nombre de personnes clés qui, chacune à leur niveau, ont contribué au succès de cette entreprise.

Je tiens à remercier en premier lieu Benoît Robert qui a vu qu'il pourrait finalement tirer quelque chose de positif du profil atypique d'un maudit français et a harcelé la direction des études de l'école pour qu'ils acceptent que me soient confiés ces travaux de recherche. Il a su m'accompagner et me conseiller tout au long de mes travaux, et m'a également permis de profiter de quelques expériences d'enseignement et de ses inévitables ... corrections. Je n'oublie pas, Benoît, que si je suis aussi vite arrivé au Québec, c'est grâce à toi.

Mes remerciements vont également à toute l'équipe du CRP avec laquelle j'ai eu beaucoup de plaisir à travailler, en particulier :

- Yannick, pour ses conseils avisés, ses commentaires toujours constructifs, et son amitié au sens large. Il m'a permis de découvrir que le Québec était aussi un pays de fromage et qu'une Alouette pesait ici plus près de 130 kg que de 130 grammes,
- Rachel, qui a supporté pendant tous ces mois – mais toujours avec moult éclats de rire - mon humour très français et mes blagues (très) sexistes,
- Luciano, pour m'avoir initié au système expert et m'avoir éclairé sur tous les aspects liés au fonctionnement des réseaux. Merci également pour tes commentaires pertinents lors de la relecture du mémoire,
- Guillaume, mon *resilience partner*, avec qui j'ai développé l'outil du futur même si aujourd'hui personne n'en a encore conscience, le « ressort de la résilience ».

J'ai également une pensée particulière pour Gilles Dusserre, de l'École des Mines d'Alès, grâce à qui tout a commencé.

Enfin, j'ai une tendre pensée pour Hannah qui m'accompagne chaque jour. Mille mercis pour ta présence, tes encouragements, ton soutien, en un mot, tout ton amour.

RÉSUMÉ

Le fonctionnement adéquat de nos sociétés repose sur la fourniture d'un certain nombre de ressources au travers des réseaux qui les supportent. Ces ressources sont fournies à la société en général mais également à d'autres réseaux en ayant besoin pour fonctionner. Typiquement, le réseau d'eau nécessite de l'électricité pour alimenter ses pompes, alors que le réseau électrique a besoin d'eau pour le refroidissement de certains équipements de production d'électricité. De telles relations de type client/fournisseur créent des interdépendances entre certains de ces réseaux. Parmi ceux-ci, ceux dont l'interruption de service aurait des conséquences sérieuses sur le fonctionnement de notre société sont catégorisés dans les infrastructures essentielles.

La fourniture adéquate de leur ressource est une préoccupation majeure et constante des opérateurs d'infrastructures essentielles. À ce titre, ils estiment devoir être capable de connaître les effets d'une défaillance initiale sur leur propre réseau ainsi que sur ceux avec lesquels il serait interconnecté. Modéliser cette propagation des défaillances dans l'espace et dans le temps, et fournir cette information au sein d'une interface conviviale leur permettrait de disposer d'un préavis utile à la mise en place de mesures de gestion destinées à limiter les conséquences d'une défaillance. Le développement d'un système d'alerte précoce s'inscrit dans cette perspective.

Les travaux de recherche présentés dans l'article en annexe ainsi que dans ce mémoire qui en détaille chacun des aspects, ont trait au développement d'un tel système en vue d'une implantation et validation à Montréal, à la fois dans sa définition, son contenu, et dans une maquette d'outil. Or, le développement du système a rencontré un certain nombre de difficultés et n'a pu être mené jusqu'à son terme. En revanche, l'examen de ses difficultés a permis d'approfondir l'analyse de la composition du système, de proposer un certain nombre de pistes permettant de contourner les obstacles rencontrés et de continuer néanmoins à utiliser ce système au travers d'autres applications, jusqu'à ce qu'une nouvelle implantation puisse être tentée.

ABSTRACT

The proper functioning of our societies lies on a certain number of key resources provided through supporting networks. These resources are provided not only to the society in general but also to other networks which use the resources the others produce. Typically, the pumps operating the water network need electricity to work, as well as the electrical network needs water to cool down certain production equipments to maintain a normal operating temperature. Such customer/supplier relationships generate interdependencies between some of these networks. Among them, some are categorized as critical infrastructures, which failure would have debilitating effects on our society.

The proper supplying of their resources is a major and permanent concern for critical infrastructure operators. As such, they consider they need to be informed of the consequences of an initial failure on their own network as well as on the ones it is interconnected with. Being able to model such propagation in space and time, and provide this information through a user-friendly interface would give operators a certain period of time within which they could take appropriate measures to mitigate the consequences. An early warning system is to be developed in this perspective.

The research presented in the article in annex as well as in this dissertation which details each of its aspects is related to the development of such a system, both in its definition, constitution and as a tool model supposed to be implemented and tested in Montreal. Thus, the development of this system faced several difficulties and could not be brought to fruition. Nevertheless, the investigation of the obstacles led to a better understanding of the constitution of the system, allowed to suggest a certain number of approaches in order to overcome them and yet to keep using the system through various applications, until a new implementation could be considered.

TABLE DES MATIÈRES

REMERCIEMENTS	III
RÉSUMÉ.....	IV
ABSTRACT	V
TABLE DES MATIÈRES	VI
LISTE DES TABLEAUX.....	IX
LISTE DES FIGURES.....	X
LISTE DES SIGLES ET ABRÉVIATIONS	XI
LISTE DES ANNEXES.....	XII
INTRODUCTION.....	1
CHAPITRE 1 REVUE DE LITTÉRATURE	4
1.1 Les systèmes d’alerte précoce	5
1.1.1 Contexte	5
1.1.2 Domaines d’application.....	5
1.2 Un cadre d’action international face aux risques naturels.....	8
1.3 Exemple de systèmes conçus pour être multirisques	10
1.3.1 Le système français d’alerte et d’information des populations.....	10
1.3.2 Le système européen ARGUS.....	12
1.4 Synthèse des éléments de littérature.....	13
CHAPITRE 2 CONTEXTE ET OBJECTIFS DE RECHERCHE	14
2.1 Contexte de recherche du CRP.....	14
2.1.1 Présentation du CRP.....	14
2.1.2 Les infrastructures essentielles.....	15
2.1.3 Les différentes interdépendances	16

2.1.4	Les définitions utilisées par le CRP	17
2.1.5	Méthodologie du CRP.....	18
2.1.6	Développement d'un système expert	23
2.2	Développement d'un SAP.....	24
2.2.1	Hypothèse de recherche	25
2.2.2	Objectifs de recherche.....	25
2.2.3	Méthodologie	26
CHAPITRE 3	DÉVELOPPEMENT DE LA MAQUETTE DU SAP	31
3.1	Cahier des charges.....	32
3.2	Définition et composantes d'un SAP	33
3.2.1	Définition	33
3.2.2	Composantes	33
3.2.3	La maîtrise des composantes.....	36
3.3	Paramètres retenus pour les visualisations	36
3.3.1	Indicateurs relatifs à la propagation de la défaillance	36
3.3.2	Indicateurs relatifs aux effets de la défaillance sur les ressources	37
3.4	Visualisations obtenues	38
3.4.1	Visualisations par indicateurs relatifs à la propagation de la défaillance	38
3.4.2	Visualisations par indicateurs d'effets	41
3.5	Prise en compte des RA	44
3.5.1	Indicateurs de niveau de fonctionnement.....	44
3.5.2	Caractérisation des RA.....	44
3.5.3	Intégration des RA dans les visualisations.....	46
3.6	Synthèse des résultats.....	49

CHAPITRE 4	DISCUSSION GÉNÉRALE	50
CONCLUSION ET RECOMMANDATIONS		62
LISTE DE RÉFÉRENCES.....		65
ANNEXE		68

LISTE DES TABLEAUX

Tableau 2.1 : Indicateur du niveau de fonctionnement d'un réseau (Robert & Morabito, 2009)...	22
Tableau 3.1 : Niveaux de fonctionnement avec ressource alternative	44
Tableau 4.1 : Synthèse des pistes de travail	54

LISTE DES FIGURES

Figure 1.1 : Les 4 éléments d'un SAP axé sur la population (UN/ISDR, 2006).....	10
Figure 2.1 : Représentation de l'état d'un système et des concepts associés (Robert, 2009)	18
Figure 2.2 : Extrait de cartographie souple utilisée par le CRP (Robert & Morabito, 2009).....	20
Figure 2.3 : Exemple d'une zone d'alimentation en ressource (télécommunications)	20
Figure 2.4 : Exemple d'une courbe de dépendance (Robert & Morabito, 2009).....	23
Figure 2.5 : Exemple de courbe générée par le système expert (Robert & Morabito, 2009).....	24
Figure 3.1 : Exemple de visualisation par ressource	39
Figure 3.2 : Exemple d'une visualisation par état.....	39
Figure 3.3 : Exemple d'une visualisation par secteur	40
Figure 3.4 : Exemple de visualisation par délai	40
Figure 3.5 : Visualisation d'effet sur les réseaux interdépendant.....	41
Figure 3.6 : Exemple de visualisation d'effet domino.....	42
Figure 3.7 : Exemple de visualisation d'effet rebond.....	43
Figure 3.8 : Exemple de visualisation d'effets cumulatifs.....	43
Figure 3.9 : Caractérisation d'une RA	45
Figure 3.10 : Dépendance à une RA	46
Figure 3.11 : Exemple d'intégration d'une ressource alternative.....	47
Figure 3.12 : Exemple de résultats	48

LISTE DES SIGLES ET ABRÉVIATIONS

CRP	Centre Risque & Performance
IE	Infrastructure essentielle
RA	Ressource alternative
SAP	Système d'Alerte Précoce

LISTE DES ANNEXES

ANNEXE 1	Article : « <i>Failures within Interdependent Systems: Challenges Related to Implementing an Early Warning System.</i> »
----------	--

INTRODUCTION

Depuis plus d'un siècle, l'industrialisation grandissante de nos sociétés a été de pair avec la création de dépendances toujours plus nombreuses à différentes ressources, dépendances à la fois individuelles et collectives s'appliquant à tous les domaines de la vie, qu'il s'agisse de la vie privée des individus, ou de la vie économique, politique et sociale des États. Chacun utilise quotidiennement un grand nombre de ces ressources et leur indisponibilité est toujours synonyme de perturbations à plus ou moins grande échelle. Plus encore, pour être fournie, certaines des ressources ont besoin d'autres ressources, créant entre elles des interdépendances plus ou moins complexes. L'électricité alimente non seulement chacune de nos maisons, nos outils de production, mais également nos moyens de transports et de communication. Les réseaux de communication ont non seulement besoin d'électricité pour fonctionner, mais également d'eau pour maintenir une température adéquate de fonctionnement. Le réseau d'eau, quant à lui, nécessite des pompes fonctionnant à l'électricité pour alimenter les résidences, les administrations, services de l'état et industries. La chaîne des interdépendances est complexe et il est facile de comprendre qu'une panne d'eau par exemple, aura des effets non seulement sur les populations, mais également sur les autres réseaux qui dépendent de cette ressource pour fonctionner. Ces interdépendances ont pour avantage de permettre à une société entière de bénéficier au quotidien des avantages liés aux différentes ressources, mais comme inconvénient majeur de générer de nouvelles et multiples vulnérabilités.

Dans un premier temps, les États ont mis en évidence que certaines de ces ressources sont critiques pour leurs populations, infrastructures et services. Elles ont été définies comme ressources essentielles, chacune étant produite, acheminée ou stockée par des infrastructures dites Infrastructures Essentielles (IE). L'identification de ces infrastructures a vu la mise en place, dans un deuxième temps, de politiques visant à les protéger et ainsi à assurer l'approvisionnement de nos sociétés en ressources. Des événements récents tels que les séismes et tsunامي au Japon en 2011, les inondations majeures en Australie en 2010, le cyclone Nargis en Birmanie en 2008 ou le « black out » électrique du Nord Est américain en 2003 témoignent du fait que nos sociétés subissent des conséquences majeures dès que leur alimentation en ressources essentielles devient défaillante.

C'est dans ce cadre que depuis une dizaine d'années, le Centre risque & performance (CRP) travaille sur les IE, en particulier sur l'évaluation de leurs interdépendances. Au travers de trois projets, le Centre a pu développer une méthodologie d'évaluation des interdépendances (Robert, De Calan, & Morabito, 2008; Robert & Morabito, 2009b; Robert, Morabito, & Quenneville, 2007), l'appliquer à Montréal et à Québec, et développer également un système expert permettant de modéliser la propagation de défaillances au sein de réseaux interdépendants (Robert & Morabito, 2010).

Les exploitants des réseaux partenaires du Centre ont reconnu que la connaissance précise de la propagation d'une défaillance dans le temps et dans l'espace était la condition de la mise en place de mesures de gestion appropriées visant à limiter cette propagation. Dans cette optique, ils ont demandé au Centre, à partir des informations fournies par le système expert, de développer un Système d'Alerte Précoce (SAP) susceptible de les informer des modalités de propagation d'une défaillance au sein de leurs réseaux, une fois une panne initiale constatée, afin qu'ils puissent mettre en place les mesures de gestion appropriées. Le développement de ce système est le sujet de ce mémoire de recherche.

Ce mémoire est destiné à approfondir et détailler le contexte de travail ainsi que les résultats qui ont été présentés au sein d'un article (disponible en annexe) qui a été soumis pour publication au *Journal of Homeland Security and Emergency Management*. Cette publication américaine couvre en effet plusieurs aspects liés aux mesures d'urgence ainsi qu'à la sécurité intérieure. L'approche que défend le CRP repose sur le fait que face à la survenue d'une possible défaillance, mieux vaut se concentrer sur la gestion des conséquences que sur ses causes, ses dernières pouvant être nombreuses, variées et plus ou moins inattendues. Les causes englobent des aléas d'origines diverses, naturelle, technologique, mais également anthropiques (erreur humaine, acte de malveillance, etc.). La gestion des conséquences, quant à elle, nécessite la mise en place de mesures d'urgence. Les résultats de ces travaux de recherche devraient donc naturellement trouver leur place dans cette publication.

Une revue de littérature mettra en évidence, dans un premier temps, que le concept d'alerte précoce n'est pas récent et qu'il s'applique, sous des formes différentes, à de nombreux domaines civils et militaires. En l'absence de définition commune, de composition standard et de références

quant à un tel système développé dans le contexte de réseaux interdépendants, elle soulignera la nécessité de définir ces éléments dans notre propre cadre de travail.

Le SAP étant vu comme une extension du système expert développé par le CRP, une présentation des travaux du Centre ainsi que des courbes générées par le système expert seront nécessaires. En effet, les travaux présentés dans ce mémoire emprunteront les concepts, les définitions et la terminologie employés par le CRP. Ces éléments de mise en contexte permettront alors de présenter la problématique et les objectifs de recherche de ce mémoire.

Dans une partie liée au développement du système, nous présenterons la définition, la caractérisation du SAP ainsi que la maquette qu'il a été possible de développer. Pour des raisons que nous exposerons, le développement n'a pas pu être mené à son terme et les travaux se sont alors orientés vers une analyse des obstacles rencontrés ainsi que vers une proposition de pistes pour d'une part, revoir le contexte d'implantation du SAP afin de contourner les difficultés identifiées, et d'autre part, dans l'attente de cette modification du contexte, de pouvoir appliquer dès maintenant l'outil développé à d'autres utilisations. Ces différents éléments feront l'objet d'une discussion générale qui ouvre la voie au développement d'outils plus adaptés aux problématiques des interdépendances entre IE.

CHAPITRE 1 REVUE DE LITTÉRATURE

Cette revue nous permet de dresser un panorama des SAP documentés dans la littérature, ainsi que de leurs différents domaines d'application.

Elle complète les différents systèmes rapidement évoqués dans l'article en annexe et permet d'illustrer que de tels systèmes sont utilisés depuis de nombreuses années dans de nombreux domaines et sous des formes multiples, car nécessairement adaptées aux contextes dans lesquels ils ont été développés. Un accent sera mis sur les SAP appliqués aux risques naturels, car, d'une part, ils bénéficient aujourd'hui d'un cadre d'action international (United Nations/International Strategy for Disaster Reduction [UN/ISDR], 2005) et, d'autre part, ils s'appliquent à des risques qui, de par leur ampleur et leur récurrence, génèrent des conséquences majeures à long terme à la fois sur les populations et les infrastructures (Emergency Events Database [EM-DAT], 2009).

Aucun écrit décrivant un SAP appliqué aux réseaux interdépendants n'a été trouvé dans la littérature. Aussi, cette revue de littérature s'attardera sur les systèmes conçus pour être multirisques, car, en l'absence de référence à des systèmes s'appliquant spécifiquement aux réseaux interdépendants, ils s'inscrivent naturellement dans la logique de l'approche de gestion des risques par conséquences défendue par le CRP.

Au Québec, il existe certaines initiatives s'apparentant plus ou moins à un SAP, comme les « *Prévisions d'un évènement météorologique perturbateur* » du Centre de Prévision des Crues du Québec (Centre de Prévision des Crues du Québec [CPCQ], 2011) capable d'évaluer les risques d'inondation, de préparer des prévisions et, s'il y a lieu, d'émettre les avertissements, ou encore le Centre d'Expertise Hydrique du Québec chargé « *d'élaborer des modèles de simulation et de prévision de débit de certains cours d'eau, de fonte des neiges et de ruissellement pour apporter, entre autres, l'expertise nécessaire à la gestion des barrages publics ainsi qu'aux intervenants de la sécurité civile en période de crue* » (Centre d'Expertise Hydrique du Québec [CEHQ], 2011). Cependant, ces systèmes ne font pas l'objet de publications scientifiques et sont mentionnés à titre d'information.

1.1 Les systèmes d'alerte précoce

1.1.1 Contexte

Accident de Tchernobyl en avril 1986, tempête Lothar en France en 1999, attentats du World Trade Center en septembre 2001, tsunami de 2004 dans l'océan Pacifique, et plus récemment, en mars 2011, tremblement de terre et tsunami au Japon, chacun constate aujourd'hui que la gestion des conséquences d'accidents d'origine naturelle ou anthropique générant des dégâts humains et/ou matériels majeurs, et susceptible de perturber sur le long terme le fonctionnement efficace d'une société, est un enjeu pour un large éventail d'acteurs privés et institutionnels.

Déjà en 2005, Ozer et de Longueville remarquaient que les catastrophes récentes alimentaient au niveau mondial une réflexion non plus simplement sur la gestion des conséquences, mais sur la possibilité de mettre en place des systèmes de gestion anticipative des risques (Ozer & De Longueville, 2005).

Pourtant, la notion même de SAP n'est pas récente, et tel Monsieur Jourdain qui s'exprimait en vers sans le savoir, les hommes ont depuis longtemps mis en place des systèmes leur permettant d'être prévenus d'un danger afin de pouvoir soit l'éviter, soit en limiter les conséquences : la sentinelle chargée de prévenir de l'arrivée de l'ennemi en est un exemple des plus anciens. Ironiquement, les oies du Capitole alertant Rome de l'attaque de Brennus en 390 avant JC en furent également un exemple efficace bien qu'involontaire.

Au fil du temps, de nombreux systèmes ont vu le jour et sont aujourd'hui utilisés dans un large éventail de domaines, à la fois civils et militaires.

1.1.2 Domaines d'application

La littérature décrit de très nombreux SAP. Leurs domaines d'application s'étendent des ouvrages de génie civil à la finance, en passant par la sécurité des populations, les crises humanitaires ou les réseaux de transport. Tous ces systèmes ont été conçus pour répondre à une problématique spécifique de risque. Les sections suivantes en présentent quelques exemples :

1.1.2.1 Exemples de systèmes à vocation civile

L'*Automatic Warning System* (AWS) est utilisé dans le transport ferroviaire britannique. Le système émet un signal à l'approche d'un panneau d'avertissement ou d'arrêt. Si le conducteur ne valide pas manuellement l'alarme, le train actionne automatiquement son système de freinage et s'arrête (Office of Rail Regulation, 2011).

Dans le domaine hydroélectrique aux États-Unis, le *Dam Safety System* (DSS) surveille, grâce au GPS et à un radar à synthèse d'ouverture, les éventuels glissements de terrain ou mouvements de subsidence pouvant mettre en péril les barrages. Parfois couplé à des sismographes, le DSS émet une alerte lorsque ses détections dépassent les tolérances prévues (Federal Emergency Management Agency [FEMA], 2004).

Au Québec, le ministère de la Santé et des Services Sociaux (MSSS) a préparé un plan « chaleur accablante », destiné à répondre aux problèmes de santé susceptibles de survenir lors d'épisodes de température minimale supérieure à 20°C et maximale supérieure à 33°C pendant une durée de 3 jours et plus. Ce plan, mis en œuvre tout au long de l'année au travers de phases de préparation, de veille, d'alerte et de mobilisation, a pour vocation à la fois à mobiliser les services publics sur la prise en charge de malades, et à informer les populations sur la conduite à tenir afin de limiter les conséquences de la vague de chaleur (Ministère de la Santé et des Services Sociaux [MSSS], 2011).

Les années 90 ont vu un grand nombre de crises financières dans les économies émergentes dont les conséquences furent majeures à la fois au niveau économique mais également politique et social. Du fait de l'interconnexion des réseaux financiers mondiaux, ces crises ne sont pas restées confinées, mais se sont propagées à d'autres marchés. Devant cet état de fait, la Banque Centrale Européenne (BCE) a développé un SAP appliqué aux crises financières afin d'identifier les faiblesses et vulnérabilités des marchés et d'anticiper les conséquences des futures crises (Bussière & Fratzscher, 2002).

Face à la vague d'attentats frappant l'Europe durant les « années de plomb » (Brigades Rouges, Bande à Baader, ...), la France décide, dès 1978, de mettre en place le plan Vigipirate destiné à « protéger la population, les infrastructures et les institutions, et préparer les réponses en cas d'attaque ». Dans sa version actuelle refondue en 2007, l'approche part du postulat que la menace terroriste est permanente et définit un certain nombre de mesures à mettre en œuvre, bien

entendu lorsque les services de l'État analysent un risque potentiel, mais également en l'absence d'informations précises sur une menace (posture de base). Il s'agit pour le gouvernement d'attirer l'attention des réseaux d'alerte et de commandement, « *d'activer les services de renseignement et de prévention* » et de mettre en place ou renforcer des mesures spécifiques en communiquant le cas échéant aux exploitants d'IE les mesures appropriées aux niveaux d'alerte correspondants (Secrétariat Général de la Défense et de la Sécurité Nationale [SGDSN], 2011).

À la suite des famines des années 80 dans le Sahel qui firent plus d'un million de victimes, les États-Unis établirent le *Famine Early Warning System* (FEWS) destiné à anticiper les futures famines et à sensibiliser les acteurs gouvernementaux sur les façons, si ce n'est de les éviter, au moins d'en limiter les conséquences. Depuis 1985, la *United States Agency for International Development* (USAID) analyse en continu, à des fins d'alerte précoce, un certain nombre d'indicateurs tels que la pluviométrie, le prix des denrées alimentaires ou les niveaux de récolte (USAID, 2011).

Enfin, lors de la Guerre Froide, les États-Unis ont développé le *Control of Electromagnetic Radiations* (CONELRAD), un système destiné aux populations civiles en réponse à une problématique militaire. Basé sur les réseaux de radio et de télévision, le CONELRAD avait notamment pour but d'alerter les populations d'une attaque de bombardiers soviétiques et de fournir un certain nombre d'informations de sécurité civile (Time Magazine, 1963). Depuis la fin de la Guerre froide, le système a été adapté aux nouveaux risques en devenant aujourd'hui un système à vocation civile, l'*Emergency Alert System* (EAS).

1.1.2.2 Exemples de systèmes à vocation militaire

Créé en 1959 à l'époque de la Guerre froide, le *Ballistic Missile Early Warning System* (BMEWS) est le premier système de détection de missiles balistiques déployé par l'armée américaine. Le réseau de détection du système, formé de 3 radars, permettait de détecter, dès son lancement, tout missile nucléaire ciblant les États-Unis, le Canada ou le Royaume Uni (Federation of American Scientists, 2011). Le réseau existe toujours aujourd'hui et a été étendu dans le cadre du programme américain « PAVE PAWS » de détection de missile et de surveillance spatiale.

De conception plus récente, le *Airborne Early Warning and Control* (AEW&C) désigne une catégorie d'avions de surveillance, de détection et de commandement intégrés au sein du concept tactique de *Command and Control Battle Management* (C2BM). Dans sa composante d'alerte précoce, le radar de l'avion opérant à très haute altitude (30 000 pieds) pendant plus de 10 heures est capable de détecter et de poursuivre simultanément sur une large zone géographique (de l'ordre de 300 000 km²) des mobiles à la fois terrestres, maritimes et aériens. L'image radar étant capturée en surplomb des zones survolées, elle permet notamment d'identifier des aéronefs circulant discrètement à très basse altitude à l'abri du relief, de déclencher une alerte et de guider des opérations d'interception des aéronefs hostiles (Organisation du Traité de l'Atlantique Nord [OTAN], 2007).

1.2 Un cadre d'action international face aux risques naturels

À la suite des conséquences de récentes catastrophes naturelles, notamment le tremblement de terre de Kobé de 1995 et le tsunami en océan Indien de 2004, la communauté internationale a tenu à Hyogo, en janvier 2005, sous l'égide de l'Organisation des Nations Unies (ONU) la Conférence mondiale sur la prévention des catastrophes.

En conclusion de cette conférence, les Nations Unies ont adopté le « *Cadre d'action de Hyogo 2005-2015 : pour des nations et des collectivités résilientes face aux catastrophes* », une démarche en 5 points visant à réduire drastiquement les pertes humaines, sociales, économiques et matérielles lors de catastrophes naturelles. La deuxième priorité d'action concerne la mise en évidence, l'évaluation et la surveillance des risques de catastrophes, ainsi que le renforcement des SAP (United Nations/International Strategy for Disaster Reduction [UN/ISDR], 2005). Les Nations Unies ont décidé de soutenir une démarche internationale visant à la mise en place de SAP sur une large échelle géographique. Ce programme a pour but d'améliorer la prévention et la résilience des communautés face à un large éventail de risques naturels tels que les sécheresses, les incendies de forêt, les inondations, les tornades, les glissements de terrain, les éruptions volcaniques et les tsunamis par l'utilisation d'une série de mesures ayant trait à une meilleure formation des populations sur la conduite à tenir en cas de survenue d'un risque naturel ainsi qu'à une diffusion rapide de l'information dans les zones considérées. Les Nations Unies estiment que de nombreuses vies auraient été épargnées lors du tsunami en océan Indien de 2004 si un SAP

avait été opérationnel dans la région, fournissant aux populations le préavis nécessaire pour se mettre à l'abri.

L'ensemble des pays participants à la conférence de Hyogo ont apporté leur soutien au développement d'un système d'alerte aux tsunamis en océan Indien, premiers prémices de la démarche internationale soutenue par les Nations Unies. Ce système est passé en phase opérationnelle 18 mois après le tsunami dévastateur (BBC News, 2006).

Les Nations Unies ont poursuivi leurs efforts par l'organisation en 2006 à Bonn de la Troisième conférence internationale sur les SAP (EWS III), au sous-titre évocateur de « *du concept à l'action* ». Cet événement a permis aux participants de faire part de leurs avancées sur des projets innovants en lien avec l'alerte précoce, d'échanger sur la possibilité de réduire les impacts des catastrophes naturelles par la mise en place de tels systèmes axés sur la population, et a vu la publication d'une « *liste de contrôle* » destinée à mettre à la disposition des organisations voulant mettre en place un SAP une « *simple liste des principaux éléments et actions auxquels les gouvernements nationaux et les organisations communautaires peuvent se référer au moment de développer ou d'évaluer des SAP, ou simplement pour vérifier que des procédures décisives sont en place.* » (UN/ISDR, 2006).

La figure 1.1 illustre les 4 éléments principaux sur lesquels les Nations Unies estiment que les SAP axés sur la santé et la sécurité des populations doivent reposer. Les travaux présentés dans ce mémoire portent sur la connaissance, la surveillance et l'alerte ainsi que la diffusion et communication du risque.



Figure 1.1 : Les 4 éléments d'un SAP axé sur la population (UN/ISDR, 2006)

1.3 Exemple de systèmes conçus pour être multirisques

Face à la multiplication des risques auxquels les populations sont exposées, la tendance actuelle est à la mise en place de systèmes conçus pour faire face, non plus à un risque spécifique, mais à une variété de risques. C'est le cas, au niveau national, du Système d'Alerte et d'Information des Populations (SAIP) français et, au niveau transnational, du système ARGUS européen.

1.3.1 Le système français d'alerte et d'information des populations

Il existe aujourd'hui un certain nombre de systèmes permettant d'alerter les populations de la survenue d'un accident imminent d'origine naturelle ou anthropique, tel que le SAIP français (Ministère de l'Intérieur, 2011).

Depuis la seconde guerre mondiale, le système d'alerte français repose sur le Réseau National d'Alerte (RNA) (Ministère de l'Intérieur et de l'Aménagement du Territoire, 2007) composé de

3800 sirènes réparties sur le territoire à proximité de lieu susceptibles de générer un risque pour les populations (barrage, usine, etc.). Ce réseau est maintenu par France Télécom, l'opérateur national de télécommunications. Ces sirènes sont susceptibles de générer deux types d'alerte sonores très distinctes associées à deux signaux sonores différents. Des campagnes d'informations organisées par les municipalités ont pour but d'informer les riverains du fonctionnement du système et des conduites réflexes à tenir selon les deux alertes :

- Un signal national d'alerte (variation du signal sur trois cycles successifs d'une durée de 1 minute et 41 secondes) demande aux riverains de se confiner et d'écouter la radio nationale pour recevoir de plus amples informations,
- Un signal de rupture de barrage (son de corne de brume sur une durée maximale de 2 minutes composée d'une émission sonore de 2 secondes entrecoupée d'un intervalle de silence de 3 secondes) demande aux riverains d'évacuer la zone d'alerte.

Le Livre Blanc de la Défense et de la Sécurité Nationale adopté en juin 2008, précise que la modernisation de l'alerte des populations est un objectif prioritaire du gouvernement et passe notamment par le remplacement du RNA par le SAIP, le premier système, maintenant plus que cinquantenaire, ne répondant plus aux enjeux actuels (Mallet, 2008). Dans le contexte de la seconde guerre mondiale, le RNA avait été initialement conçu pour avertir les populations d'un risque de bombardement. Aujourd'hui, face aux nombreux risques naturels, technologiques ou terroristes auxquels les populations sont exposées, le gouvernement français a décidé de développer un système multirisque à la fois d'alerte et d'information.

Le SAIP, développé par la Direction de la Sécurité Civile, part du principe qu'il existe un certain nombre de bassins de risques au sein desquels seront déployés et mis en œuvre les moyens d'alerte les plus efficaces eu égard à l'environnement : selon le degré d'urbanisation, le bruit ambiant et le type de population à alerter, un large éventail de moyens pourront être déclenchés indépendamment ou ensemble, tels que des sirènes, des automates d'appel, des panneaux à messages variables ou de la messagerie vers les téléphones mobiles par exemple. Destiné à répondre au plus large panel de risques possible, naturels (inondations, séismes, etc.), technologiques (incendies, explosions, accident de matières dangereuses, etc.) ou terroristes, le SAIP intègre à la fois une fonction d'alerte et d'information :

- D'alerte, car il est destiné à avertir la population d'un danger imminent et à générer une conduite à tenir réflexe,
- D'information, car l'emploi de systèmes de communication permet de tenir la population informée du développement de l'évènement et des conduites appropriées sur le plus long terme.

La mise en œuvre du SAIP fait l'objet d'un programme de déploiement s'étalant de 2009 à 2015 (Ministère de l'Intérieur, 2011).

1.3.2 Le système européen ARGUS

Suite aux attentats de Madrid en 2004, la Commission Européenne s'est interrogée sur la meilleure façon d'améliorer sa coordination interne en cas de crise multisectorielle. L'une de ses recommandations a été la mise en place d'une plateforme Web d'échange d'information et d'alerte mise en ligne en 2006 sous le nom d'ARGUS.

ARGUS est un système central créé par la communauté européenne «... *afin de renforcer ses capacités d'intervenir d'une manière rapide, efficace et coordonnée, face à une crise de nature multisectorielle, quelle qu'en soit la cause, affectant plusieurs secteurs et réclamant une action au niveau communautaire.* » (Commission des Communautés Européennes, 2005).

ARGUS a pour but de fournir un support rapide d'échange d'informations entre les différentes directions de la Commission Européenne. C'est également un moyen de liaison entre autorités politiques permettant une coordination efficace en cas de crise multisectorielle. Il prend la forme d'une plateforme Web d'échange d'information alimentée par plusieurs systèmes d'alerte spécifiques à des risques particuliers (Kjellén, 2009), entre autres :

- Le *Common Emergency Communication and Information System* (CECIS), reliant les autorités chargées de la sécurité civile et des pollutions maritimes,
- Le *European Community Urgent Radiological Information Exchange* (ECURIE), pour les alertes de type Chimique, Biologique, Radiologique, Nucléaire et Explosif (CBRNE),
- L'*Early Warning and Response System* (EWRS), pour les risques liés aux maladies contagieuses,
- Le *Rapid Alert System for Food and Feed* (RASFF) pour les risques alimentaires,

- Le *Critical Infrastructure Warning Information Network*), CIWIN pour les risques liés aux IE.

Les conséquences des attentats de Londres en 2005 ont vu, à la demande du Conseil de l'Europe, la mise en place de plusieurs initiatives visant à l'amélioration de la gestion de crise telles que la création d'un manuel européen d'urgence et de coordination de crise (*Manual on EU Emergency and Crisis Coordination*).

1.4 Synthèse des éléments de littérature

Les différentes ressources à disposition dans la littérature mettent en évidence que les SAP n'ont ni forme ni composantes universelles et qu'ils ne se conçoivent que s'ils répondent aux besoins d'un environnement connu.

Il n'existe pas non plus de définition universelle d'un SAP, chaque organisation à l'origine d'un développement en donnant sa propre définition selon les objectifs pour lesquels le système aura été conçu.

Ce que montre cependant la multiplicité des systèmes en vigueur aujourd'hui, c'est la nécessité pour l'homme d'être capable d'être prévenu rapidement d'un changement potentiellement néfaste de son environnement. Que se soit pour les décideurs qui exploitent le générateur de risque, les industriels par exemple, les gouvernements qui sont responsables de leurs administrés ou bien les individus eux-mêmes, ces systèmes reposent sur la possibilité de disposer d'un délai suffisant soit pour maîtriser le changement et éviter qu'il ne provoque des conséquences négatives, soit pour prendre des mesures de protection lorsque le changement est survenu.

Aussi, alors qu'il faudra développer de toutes pièces, en l'absence de précédents, un SAP appliqué aux réseaux interdépendants, il sera nécessaire, à partir d'une définition qui illustrera l'objectif du système, d'en définir à la fois la forme et la composition afin qu'il réponde aux besoins de la problématique spécifique des interdépendances.

CHAPITRE 2 CONTEXTE ET OBJECTIFS DE RECHERCHE

Le développement d'un SAP appliqué aux réseaux interdépendants s'inscrit dans le contexte de recherche du CRP.

Le Centre, au travers de plusieurs projets en partenariat avec la Sécurité civile et les exploitants d'IE, a récemment développé un système expert permettant de modéliser les effets de la propagation d'une défaillance au sein des différents réseaux étudiés.

Le SAP, aboutissement du dernier projet en cours, se veut être une extension du système expert permettant de fournir aux partenaires un outil d'information et d'alerte sur la propagation de ces défaillances.

2.1 Contexte de recherche du CRP

2.1.1 Présentation du CRP

Le CRP a développé depuis une dizaine d'années une démarche d'étude des interdépendances entre IE au travers de 3 projets principaux :

- Le premier projet, débuté en 2005 et échelonné sur une période de 3 ans, consistait à développer une méthodologie d'identification et d'évaluation des interdépendances et des effets domino entre réseaux de support à la vie appliquée à la ville de Montréal. Ce projet a vu la publication d'un guide méthodologique développant une méthodologie permettant d'évaluer les interdépendances entre les réseaux interdépendants et de mettre en place des outils de gestion adaptés (Robert & Morabito, 2009b).
- Le second, conduit en 2006 et 2007, a consisté en l'application et la validation de cette même méthodologie à la ville de Québec.
- Le troisième, débuté en 2008 et se poursuivant jusqu'en 2012, a pour but de développer un système expert permettant de modéliser la propagation de défaillances au sein de réseaux interdépendants. À ce système expert devra s'adjoindre un SAP permettant aux

exploitants d'infrastructures de mettre en place des mesures de gestion et d'atténuation efficaces en cas de défaillance (Robert, et al., 2008).

Le CRP travaille en partenariat à la fois avec les bureaux de Sécurité Civile de Montréal et de Québec ainsi qu'avec un certain nombre d'exploitants d'IE : électricité, gaz naturel, télécommunications, transport et eau potable.

2.1.2 Les infrastructures essentielles

Au Canada, les IE se définissent comme « *les processus, les systèmes, les installations, les technologies, les réseaux, les biens et les services qui sont essentiels à la santé, à la sécurité ou au bien-être économique des Canadiens et des Canadiennes, ainsi qu'au fonctionnement efficace du gouvernement* ». Elles sont réparties en 10 catégories (Sécurité Publique Canada, 2010) :

- L'énergie et les services publics (systèmes de production d'énergie électrique, de gaz naturel et de pétrole ainsi que leurs réseaux de transport),
- Les technologies de l'information et de la communication (systèmes, logiciel, matériel et réseaux de télécommunications et de radiodiffusion, incluant Internet),
- Les finances (opérations bancaires, valeurs mobilières et investissements),
- La santé (hôpitaux, établissements de soins de santé et de réserve de sang, laboratoires et produits pharmaceutiques),
- L'alimentation (sécurité, distribution, agriculture et industrie alimentaire),
- L'eau (eau potable et gestion des eaux usées),
- Les transports (voies aériennes, ferroviaires, maritimes et terrestres),
- La sécurité (sécurité contre les armes chimiques, biologiques, radiologiques et nucléaires, matières dangereuses, recherche et sauvetages, secours d'urgence),
- Le gouvernement (services, installations, réseaux d'information, biens gouvernementaux, sites et monuments nationaux privilégiés),
- Le secteur manufacturier (industries liées à la fabrication de biens)

La définition et le périmètre des IE est variable selon chaque pays. Aux États-Unis par exemple, elles se définissent comme les “*assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof*”, et se déclinent en 18 catégories (agriculture et alimentation, banques et finances, industrie chimique, communication, industrie critique, barrages, industrie de défense, services d’urgence, énergie, infrastructures gouvernementales, soins et santé publique, technologies de l’information, monuments nationaux, réacteurs, matériels et déchets nucléaires, services de la Poste et expédition de biens, systèmes de transport et eau) (Department of Homeland Security [DHS], 2009).

2.1.3 Les différentes interdépendances

L’échange d’informations ou de ressources entre IE suppose qu’il existe entre elles un certain niveau de dépendance (échange dans un sens) ou d’interdépendance (échange réciproque). Les interdépendances entre IE sont au nombre de 4 (Rinaldi, Peerenboom, & Kelly, 2001) :

- Les **interdépendances physiques** (ou **fonctionnelles**) supposent qu’il y ait un échange direct de ressources entre IE, chacune ayant besoin de l’autre pour fonctionner. Par exemple, la distribution d’eau nécessite des pompes alimentées par l’électricité. A l’inverse, le refroidissement des systèmes électriques est réalisé grâce à l’eau.
- Les **interdépendances géographiques** supposent une proximité entre IE. Par exemple, l’explosion d’une conduite de gaz enterrée peut entraîner une interruption d’eau dès lors que les canalisations de gaz et d’eau suivent le même trajet.
- Les **interdépendances cybernétiques** caractérisent l’échange d’informations entre infrastructures. Dans l’exemple des *Supervisory Control and Data Acquisition* (SCADA), le contrôle à distance est réalisé grâce au réseau de télécommunications.
- Les **interdépendances logiques** caractérisent la relation entre plusieurs IE lorsque l’état de chacune est fonction de l’état des autres en l’absence de lien fonctionnel, géographique ou cybernétique. Par exemple, les troubles sociopolitiques du printemps 2011 en Afrique du Nord et au Moyen Orient ont provoqué une augmentation du prix du baril de pétrole (Agence France Presse [AFP], 2011).

Les travaux du CRP se sont concentrés sur les interdépendances fonctionnelles et géographiques (Robert, et al., 2008; Robert & Morabito, 2010) et ont vu le développement d'outils permettant :

- D'identifier, de caractériser et de hiérarchiser les interdépendances entre IE,
- D'identifier et d'anticiper la propagation d'effets domino,
- De mettre en place des mesures de prévention et de protection.

2.1.4 Les définitions utilisées par le CRP

Afin de faciliter la compréhension de ses travaux, le CRP a défini un certain nombre de concepts. Le développement d'un SAP appliqué aux réseaux interdépendants a fait appel à certains d'entre eux (Robert, 2009) :

- **Aléa** : événement perturbateur qui peut modifier l'état d'un système. L'aléa peut être interne ou externe.
- **Conséquence** : effet, évolutif dans le temps, sur le ou les utilisateurs, des défaillances d'un système.
- **Défaillance** : altération ou dégradation de l'état du système.
- **État d'un système** : caractérisation de l'aptitude d'un système, évolutive dans le temps, à accomplir sa ou ses missions requises avec les performances spécifiées et acceptables.
- **Effet domino** : réaction en chaîne au cours de laquelle une cause initiale de défaillance produit un effet chez une entité d'un espace de coopération et qui, à son tour, se répercute sur une autre entité en raison de l'interdépendance entre elles.
- **Risque** : combinaison de la vulnérabilité d'un système et des aléas susceptibles d'engendrer des conséquences.
- **Système** : ensemble cohérent d'éléments (ou de processus) liés par des objectifs, des responsabilités ou de missions communes et fixées.
- **Vulnérabilité** : propriété, évolutive dans le temps, d'un système à subir des défaillances en fonction de son état.

La figure 2.1 présente l'état de fonctionnement d'un système ainsi que les différents concepts qui s'y rattachent. Soumis à un aléa, l'état d'un système risque d'être suffisamment perturbé pour quitter un mode de fonctionnement normal vers un mode perturbé voire défaillant. Ces états seront susceptibles de générer des conséquences à l'extérieur des frontières du système, sur son environnement. Le risque peut alors se comprendre comme l'ensemble de la figure, c'est-à-dire la combinaison de l'aléa, du système en lui-même caractérisé par sa vulnérabilité, et des conséquences engendrées.

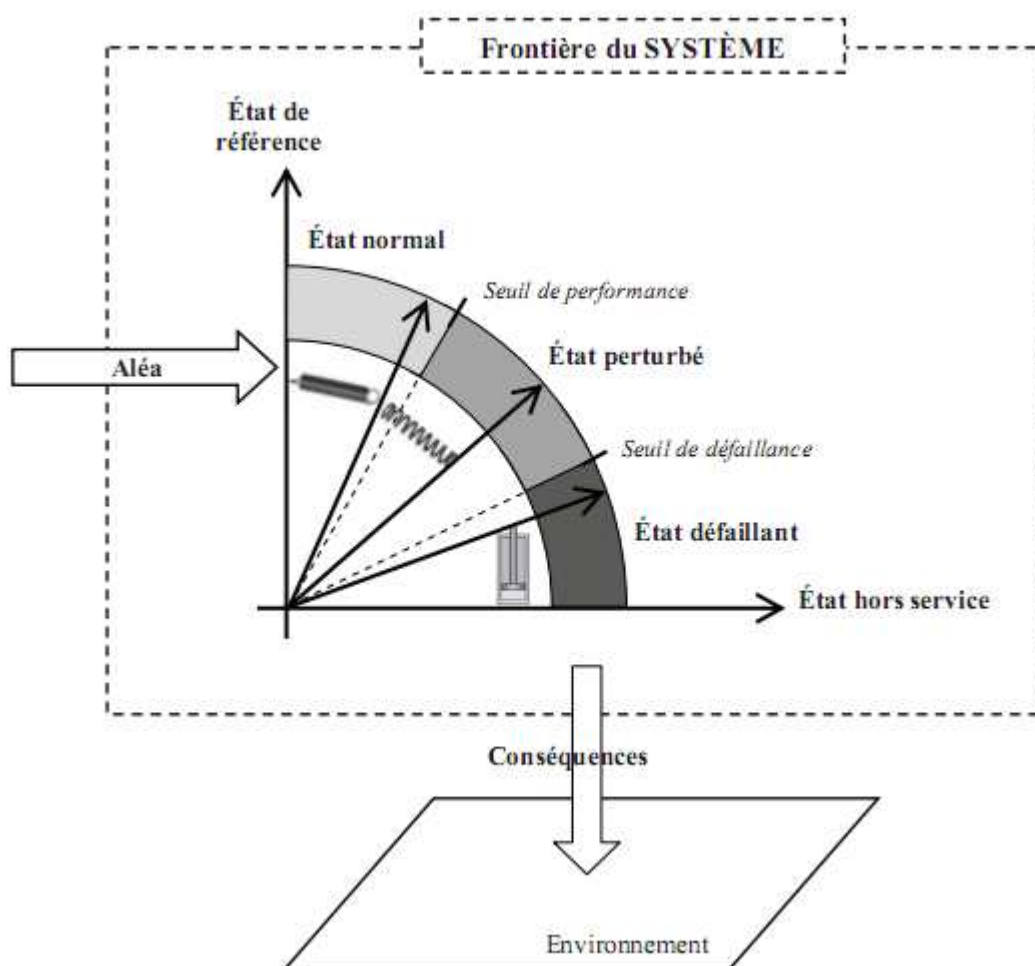


Figure 2.1 : Représentation de l'état d'un système et des concepts associés (Robert, 2009)

2.1.5 Méthodologie du CRP

Afin d'évaluer et de modéliser les interdépendances entre IE, la méthodologie du CRP repose sur une démarche en 5 étapes (Robert & Morabito, 2009b) :

1. La définition de l'espace de coopération

Comme illustré dans la figure 2.1, l'étude des interdépendances ne se conçoit que si les frontières du système sont établies. Ces frontières sont les limites de *l'espace de coopération*, formé des exploitants d'IE participant à l'étude. Parfaitement identifiés et travaillant dans un cadre de confidentialité discuté au préalable, ces acteurs sont à même de partager les informations nécessaires à l'étude. Lors de réunions régulières leur est présenté l'état d'avancement des travaux auquel ils contribuent en validant ou en commentant les différents résultats obtenus. Première étape de la méthode, la définition de l'espace de coopération se décline selon une démarche en 6 points allant de la définition des objectifs de l'étude à la gestion de la confidentialité.

2. La caractérisation de la zone d'étude

Cette étape rassemble l'information géographique nécessaire à l'étude des interdépendances. Ces informations sont de 2 sortes :

- Une sectorisation de la zone d'étude.

Afin de rendre lisibles les informations relatives à la propagation géographique d'une défaillance, les membres de l'espace de coopération partagent une cartographie commune de la zone d'étude, sous forme d'un quadrillage superposé à une carte géographique de la zone. Le quadrillage est arbitraire mais doit rester lisible. Il doit donc être préférablement orienté dans l'espace selon les points cardinaux et avoir une taille raisonnable, ni trop grande sans quoi les résultats seraient trop généraux, ni trop petite au risque de résultats trop ponctuels. Le CRP a opté pour un quadrillage de 1km x 1km (figure 2.2), qu'il baptisera *cartographie souple*. Cette cartographie permet de respecter la confidentialité des données dans la mesure où les infrastructures ne sont pas précisément localisées (Robert, et al., 2007).

- Les zones d'alimentation en ressources

Les zones d'alimentation en ressources sont des données techniques propres à chaque réseau. En général, chacune des infrastructures d'un réseau alimente en ressource une zone géographique définie. Il est demandé alors à chaque partenaire d'identifier ses propres zones d'alimentation (figure 2-3) et de partager cette information avec les autres membres de l'espace de coopération.



Figure 2.2 : Extrait de cartographie souple utilisée par le CRP (Robert & Morabito, 2009)



Figure 2.3 : Exemple d'une zone d'alimentation en ressource (télécommunications)
(Robert & Morabito, 2009)

3. *La caractérisation des IE*

Cette étape permet de connaître l'architecture d'un réseau et de comprendre son fonctionnement de manière à la fois globale (dans son ensemble) et spécifique (dans les limites de la zone d'étude).

La caractérisation globale vise à comprendre à la fois la structure et le fonctionnement général d'un réseau. Les informations nécessaires seront recueillies par le biais d'un formulaire développé par le CRP et renseigné par l'exploitant de chaque réseau. Elles comprendront le type de mission (c'est-à-dire le type de ressource concernée), les fonctions (production, transport, stockage ...), le nom et le numéro d'identification de l'ensemble des infrastructures assurant la fonction ainsi que le nom de l'entité responsable de son fonctionnement. Ces informations seront susceptibles d'être partagées entre plusieurs zones géographiques différentes. Par exemple, Hydro-Québec alimentant l'ensemble de la province, la caractérisation globale de son réseau sera la même que l'étude soit menée à Montréal ou à Québec.

La caractérisation spécifique va, quant à elle, permettre de rassembler les informations nécessaires au fonctionnement d'un réseau dans la limite de la zone d'étude. Ces informations seront également recueillies par le biais d'un questionnaire et comprendront l'identification des différentes infrastructures présentes dans la zone d'étude, leur localisation, et les conséquences de la défaillance de chaque infrastructure sur l'état du réseau.

4. *L'analyse des interdépendances*

À partir des informations recueillies précédemment, cette étape permettra de mettre en évidence les différentes interdépendances fonctionnelles et géographiques qui relient les IE de la zone d'étude.

Les travaux les plus aboutis ont aujourd'hui trait aux interdépendances fonctionnelles puisqu'ils ont permis d'établir des courbes de dépendances des ressources entre elles, illustrant pour chacun des réseaux interdépendants les effets d'une défaillance initiale (Robert & Morabito, 2009b).

Afin d'établir ces courbes de dépendances développées plus loin, il aura été au préalable nécessaire d'identifier pour chaque réseau :

- les **ressources** qu'il utilise

On identifiera à la fois les ressources courantes qu'il utilise pour fonctionner et les ressources alternatives disponibles en cas de fonctionnement en mode dégradé. Par exemple, une infrastructure peut utiliser de l'électricité pour fonctionner de façon courante et du diesel pour faire fonctionner des génératrices de secours en mode dégradé.

- les **conséquences** et le **niveau de tolérance** du réseau à la dégradation d'une ressource.

Pour chacune des ressources utilisées, on identifiera les conséquences de la dégradation de cette ressource sur le fonctionnement du réseau ainsi que le niveau de perturbation de la mission du réseau en cas de dégradation de la ressource utilisée.

Les différents niveaux de tolérance du réseau à la dégradation d'une ressource sont illustrés dans le tableau 2.1.

Indicateur	Description
Vert	Le réseau fonctionne normalement avec les ressources qu'il utilise de manière courante ou sans l'apport d'une ou plusieurs ressources courantes.
Jaune	Le réseau utilise une ressource dégradée à l'une ou plusieurs de ses infrastructures et met en place des moyens ou des ressources alternatives pour compenser la dégradation de la ressource sont suffisantes. La mission du réseau est maintenue à long terme.
Orange	Le réseau utilise une ressource dégradée à l'une ou plusieurs de ses infrastructures et les moyens ou ressources alternatives mis en place pour compenser la dégradation de la ressource ne sont pas suffisants. La mission du réseau est compromise à court terme.
Rouge	La mission du réseau est affectée sur un ou plusieurs secteurs dans la zone d'étude. La ressource n'est plus fournie dans ces secteurs.

Tableau 2.1 : Indicateur du niveau de fonctionnement d'un réseau (Robert & Morabito, 2009)

5. La mise en place d'outils de gestion

La compilation et la combinaison des différentes informations fournies par les réseaux ont permis de développer 3 outils de gestion : les courbes de dépendances, les courbes de ressources alternatives et les courbes d'effets domino (Robert & Morabito, 2009b).

L'accent sera mis sur les courbes de dépendances puisque ce sont elles que nous utiliserons dans le projet de recherche lié au développement d'un SAP.

Les courbes de dépendance permettent d'illustrer l'effet sur différents réseaux interdépendants de la dégradation de la fourniture d'une ressource initiale. Ces courbes se lisent pour une zone géographique donnée.

La figure 2.4 illustre l'impact sur 5 réseaux interdépendants les conséquences d'une défaillance initiale en eau. La zone géographique donnée est appelée *zone d'étude*. L'échelle de temps est représentée en abscisse et les réseaux en ordonnée. Alors que le réseau 3 n'est absolument pas touché par la panne, on constate que les réseaux 4 et 5 vont être perturbés dans le temps alors que les réseaux 1 et 2 vont subir tous les états de dégradation jusqu'à la défaillance complète. Le code couleur utilisé pour illustrer les différents états des réseaux est indiqué dans le tableau 2-1.

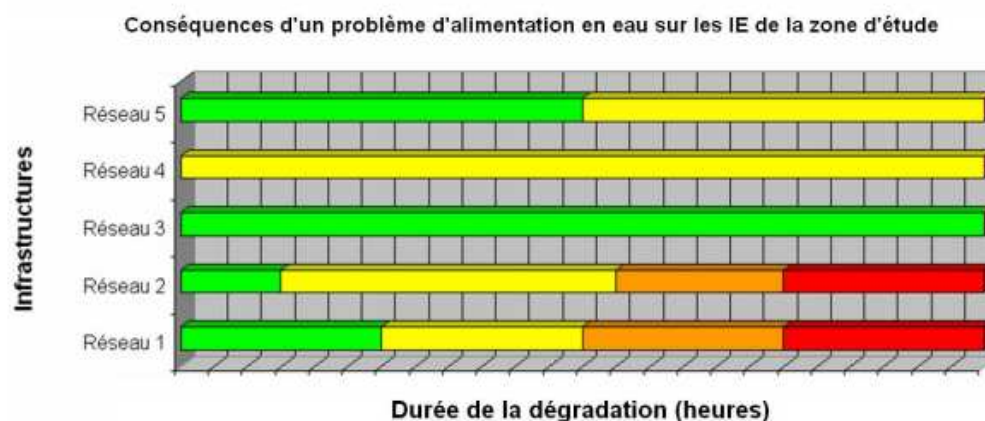


Figure 2.4 : Exemple d'une courbe de dépendance (Robert & Morabito, 2009)

Ces courbes de dépendances donnent de l'information précieuse aux exploitants de réseaux. Elles permettent d'identifier quels réseaux interdépendants vont subir une dégradation suite à une panne dans un réseau initial et fourniront également une information de délai permettant aux exploitants de disposer d'un préavis utile à la mise en œuvre de mesures de gestion adaptées.

2.1.6 Développement d'un système expert

Le mandat du projet en cours est de développer un système expert de modélisation des interdépendances et un SAP associé.

Le système expert, baptisé *Domino*, est aujourd'hui fonctionnel. Les informations fournies par les exploitants de réseaux ont été rassemblées au sein d'une base de données MS Access© et permettent de générer automatiquement les courbes de dépendance.

Ces courbes sont du même format que celle présentée en figure 2.4 et conservent comme référence géographique le quadrillage habituellement utilisé par le Centre (figure 2.2).

Domino permet par exemple (figure 2.5) de déterminer automatiquement qu'une panne initiale d'eau dans un secteur donné (AH-23) aura des conséquences majeures allant jusqu'à l'interruption de service dans les réseaux de télécommunications qui engendrera à son tour la fermeture d'un axe routier majeur par le non fonctionnement de ses systèmes de surveillance à distance.

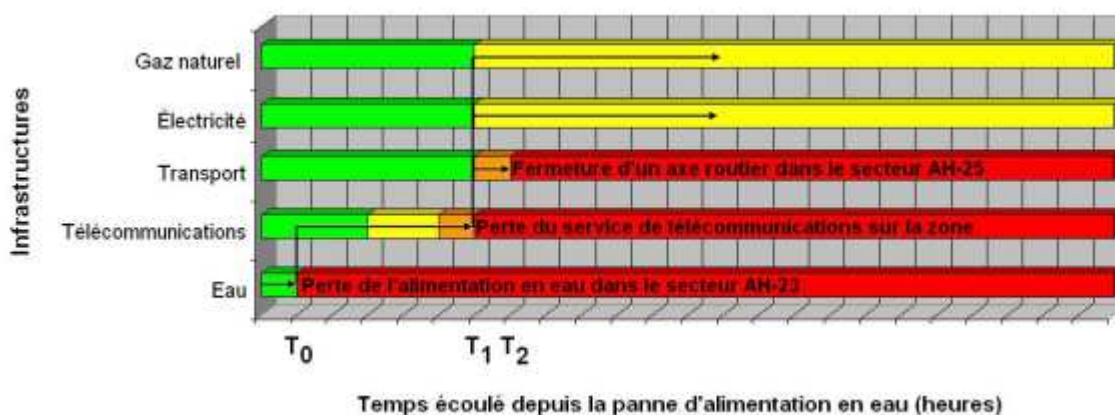


Figure 2.5 : Exemple de courbe générée par le système expert (Robert & Morabito, 2009)

2.2 Développement d'un SAP

Le développement d'un SAP appliqué aux réseaux interdépendants fait partie du projet 2008-2012 du CRP et s'y intègre comme une extension du système expert.

Dans le cadre de ce projet de recherche, une maquette de SAP a pu être développée mais son implantation à Montréal pour opérationnalisation et validation n'a pas pu être menée à bien. Ce processus a en effet fait face à des difficultés amenant à reconsidérer la pertinence de l'outil en tant que tel, mais également le concept même de SAP appliqué aux réseaux interdépendants. Le

détail de ces travaux ainsi que les conclusions auxquelles ils aboutissent sont détaillées dans l'article en annexe.

2.2.1 Hypothèse de recherche

L'hypothèse qui devait être validée ou infirmée lors de ce projet de recherche était qu'un SAP permettait d'améliorer significativement la qualité et le délai de réponse aux défaillances se propageant au sein des réseaux interdépendants.

En termes de qualité, le SAP doit permettre aux opérateurs de réseaux d'anticiper les conséquences d'une défaillance initiale en les alertant sur la propagation géographique et temporelle des conséquences afin qu'ils puissent mettre en œuvre des moyens techniques visant soit à limiter la propagation de ces effets, soit à pallier la dégradation d'une ou plusieurs ressources par l'utilisation de ressources alternatives préalablement identifiées.

En termes de délai, le SAP doit informer les opérateurs de réseaux de la survenue d'un éventuel délai critique au-delà duquel l'approvisionnement en ressources essentielles, en mode de fonctionnement normal ou grâce à l'emploi de ressources de secours, est compromis.

L'originalité de ce projet réside dans le fait que les opérateurs d'IE interviennent aujourd'hui en mode uniquement réactif car ils ne disposent pas d'outil leur permettant d'anticiper les conséquences de défaillances se propageant au sein de leurs réseaux.

L'hypothèse serait réfutée si la réponse aux défaillances d'IE n'est pas significativement plus rapide et plus efficace avec l'outil que dans les simulations sans SAP.

2.2.2 Objectifs de recherche

L'objectif général de ce projet de recherche consiste à développer une maquette d'outil opérationnel d'aide à la décision (le SAP) au profit des opérateurs d'IE en cas de survenue d'une défaillance au sein de réseaux interdépendants.

Dans une première phase, il s'agit de caractériser les modes actuels de réponse des opérateurs d'IE aux défaillances des réseaux. Au travers d'échanges et des informations disponibles dans le système expert, les informations permettant de répondre plus rapidement et plus efficacement aux défaillances de leurs réseaux peuvent être identifiées.

Dans une deuxième phase, il est nécessaire de développer le SAP proprement dit sous la forme d'une interface cartographique et informationnelle (maquette) fournissant sous un format convivial les informations requises sensées permettre de mieux répondre aux défaillances. Il sera nécessaire de définir des ressources, délais et secteurs géographiques critiques sur lesquels attirer particulièrement l'attention des opérateurs.

Dans une troisième phase, nous pourrons déterminer les délais et l'efficacité de réponse à des défaillances simulées avec et sans l'utilisation du SAP.

Enfin, dans une quatrième phase, l'outil pourra être amélioré et validé au travers d'un exercice final grâce aux commentaires des opérateurs recueillis en phase 2 et des résultats obtenus en phase 3.

Ces deux dernières phases n'ont pas pu être développées pendant le travail de recherche comme exposé plus loin.

2.2.3 Méthodologie

La méthodologie retenue a été dans un premier temps de collecter un certain nombre d'informations à la fois dans la littérature et auprès des opérateurs de réseaux. Ensuite, à partir de ces informations combinées à celles fournies par le système expert, il a été possible de définir un cadre de développement et de validation du SAP propre à notre problématique.

1. Collecte d'informations

La collecte des informations nécessaires au projet s'est faite au travers de 2 axes.

Le premier a consisté en une revue de littérature sur les systèmes essentiels et les différents types de SAP développés à travers le monde sur différents types de problématiques. Cette revue a montré la diversité des systèmes mais également qu'aucun d'entre eux n'avait spécifiquement été développé pour répondre à la problématique des réseaux interdépendants.

Le second a consisté en la définition des besoins des partenaires. En étudiant avec eux les modes actuels de réponse aux défaillances de leurs réseaux, il a été possible de mettre en évidence un certain nombre d'informations dont ils ne disposent pas de façon évidente aujourd'hui et dont ils

auraient besoin afin d'anticiper les effets d'une défaillance. Il s'agit d'indicateurs pertinents à faire figurer dans l'interface visuelle du SAP.

2. Caractérisation des modes actuels de réponse aux défaillances

Les opérateurs de réseaux ne disposent pas aujourd'hui d'un outil leur permettant d'anticiper sur la survenue d'une défaillance au sein de leurs réseaux. Ils travaillent donc en mode réactif, en subissant la défaillance, en observant sa propagation et en intervenant ponctuellement au sein de leur propre réseau afin de tenter d'en limiter les effets.

Les IE étant par nature interconnectées (par exemple, un répartiteur téléphonique aura besoin d'électricité pour fonctionner et d'eau pour maintenir à température de fonctionnement ses composants électroniques), une défaillance dans un réseau initial a de très fortes chances de se propager dans d'autres réseaux. Grâce aux travaux du CRP, les opérateurs disposent aujourd'hui du système *Domino* permettant de créer des courbes de dépendance de réseaux essentiels. Bien que ces courbes traduisent les interdépendances entre les réseaux, elles ne permettent pas de fournir de l'information pertinente à la mise en œuvre d'actions permettant d'anticiper les effets de défaillances au sein des réseaux, ni sur la survenue de la défaillance initiale.

Au travers de l'observation des modes de réponse actuels et du recueil des besoins des opérateurs, ce sont ces informations qui ont précisément été identifiées et retranscrites au sein d'un outil de visualisation convivial et performant.

3. Développement du SAP

Le développement du SAP, pour être complet, doit suivre la chronologie en 6 étapes suivantes. Comme mentionné en introduction du chapitre, le développement technique n'a pas pu être mené à son terme et a été interrompu avant l'étape 4. Nous pouvons néanmoins présenter à la fois les étapes terminées, et les étapes restant à compléter pour le développement complet du SAP.

Les étapes complétées

1. Analyse des informations à faire apparaître au sein du système

À partir des informations collectées, il a fallu définir la façon dont ces informations pouvaient être agrégées afin d'être disponibles au sein du système de manière rationnelle et efficace. En effet, fournir de l'information efficace ne consiste pas en l'intégration de l'ensemble de l'information disponible en ordre dispersé au sein du système, mais en l'analyse et le recoupement de ces informations de façon à ce qu'elles puissent être présentées de façon pertinente, selon un certain nombre de requêtes initiales liées à la propagation de la défaillance.

La hiérarchisation de ces informations a permis de faire ressortir un certain nombre d'éléments jugés critiques en termes de ressource, de secteur géographique ou de délai qu'il faut identifier de façon toute particulière afin que les opérateurs de réseau puissent y concentrer leurs efforts.

2. Détermination du type de visualisations adaptées

Une fois agrégées, ces informations ont dû être disponibles pour les opérateurs dans un ou plusieurs modes de visualisation adaptés.

Certaines de ces informations sont liées aux ressources elles-mêmes, ressources initiales ou ressources alternatives (par exemple, électricité fournie par le réseau vs. groupe électrogène), alors que d'autres sont liées à la propagation géographique de la défaillance, ou d'autres encore aux différents délais avant que différentes défaillances ne surviennent au sein de différents réseaux. Ces informations ont pu être, selon le cas, traduites sous forme de diagrammes, de courbes ou encore de cartes.

Il convient donc déterminer et de créer les visualisations pertinentes en fonction des informations à délivrer.

3. Choix de l'interface cartographique supportant ces informations

Le CRP dispose aujourd'hui d'outils de visualisation sous MS Access® et MS Excel®.

Il a semblé pertinent de conserver l'un de ces supports dans la mesure où les informations liés aux structures et interconnexions de réseaux y ont déjà été enregistrées. Le transfert d'information entre outils en a été facilité. En particulier, le Centre dispose d'un outil de cartographie de la ville de Montréal sous MS Excel® permettant d'isoler visuellement des secteurs géographiques particulier selon certaines requêtes programmées sous forme de macros en langage Visual Basic.

Pour autant, le choix de l'interface finale reposera essentiellement sur les besoins en visualisation d'information. Au cas où aucun des supports précédents ne s'avèrerait adapté, il sera nécessaire d'étudier la possibilité de transférer les informations déjà enregistrées dans une nouvelle interface du SAP.

Les étapes restant à compléter

4. Programmation de l'interface

Les interfaces visuelles ont été développées manuellement. Afin de parfaire le système, il serait intéressant, dans un deuxième temps, de s'adjoindre les services d'un informaticien afin d'obtenir conseil sur la faisabilité des différentes visualisations nécessaires en fonction des différents logiciels disponibles, et, qu'ensuite, il puisse procéder à la programmation de l'interface retenue.

5. Comparaison des réponses

Une fois le prototype du SAP programmé, il sera nécessaire de conduire, en collaboration avec les partenaires, plusieurs simulations et leur permettre d'y répondre d'abord sans le SAP, puis avec le SAP.

Il faudra ensuite s'attacher à qualifier d'une part les délais de réponse et d'autre part la qualité des réponses. L'utilisation de l'outil devra permettre d'augmenter significativement ces deux facteurs par rapport à une réponse sans outil, telle qu'aujourd'hui. Les délais se mesureront en termes de temps, alors que la qualité se mesurera dans la facilité à maintenir l'approvisionnement en ressources potentiellement défaillantes.

6. Validation de l'outil

Grâce à une approche itérative, l'outil pourra être développé en collaboration étroite avec les opérateurs de réseaux qui seront à même, à chaque étape, de formuler commentaires, souhaits ou avis sur son développement. Le prototype final devrait donc être très proche des souhaits des opérateurs.

Pour autant, seul un exercice final avec ce prototype nous permettra soit de valider d'emblée l'outil, soit d'y apporter les dernières améliorations nécessaires à son passage en phase opérationnelle.

CHAPITRE 3 DÉVELOPPEMENT DE LA MAQUETTE DU SAP

La réponse aux défaillances est une préoccupation majeure et constante des opérateurs d'IE. À cet égard, il paraît intéressant qu'ils puissent disposer d'un outil d'anticipation leur permettant de réagir rapidement et efficacement aux possibles défaillances de leur réseau. Cet outil d'aide à la décision doit leur permettre :

- D'une part de visualiser dans l'espace et dans le temps la propagation d'une défaillance initiale,
- D'autre part d'identifier, selon cette défaillance initiale, de possibles ressources, secteurs géographiques et délais critiques,
- Et enfin doit leur proposer la mise en œuvre de mesures de gestion visant à limiter les conséquences de la défaillance ainsi que des Ressources Alternatives (RA) pertinentes permettant de pallier les dégradations en garantissant la poursuite de l'approvisionnement en ressources essentielles de la population, mais également des autres systèmes interdépendants.

Comme la revue de littérature l'a mentionné, il n'existe aucun outil similaire documenté aujourd'hui. Aussi la définition complète d'un SAP, de ses objectifs à ses composantes et visualisations, ont été entièrement définies pendant le projet de recherche.

Une maquette de SAP sous format MS Excel© a pu être développée. Les informations présentées par cette maquette ont été introduites manuellement. Une deuxième étape de développement, comme évoqué dans le chapitre précédent, devrait être une automatisation des visualisations du SAP.

La maquette a été développée en 2 temps :

- Un premier, sans la prise en compte de RA, la ressource étant soit disponible, soit indisponible,
- Un deuxième, avec la prise en compte de RA, amenant à une modification du code de couleurs (tableau 2.1) concernant l'état de la ressource.

Cette maquette est également présentée dans l'article en annexe et supporte un certain nombre de réflexions liées à la conception de l'outil. Ces réflexions ont permis de comprendre certaines des raisons pour lesquelles le SAP tel que développé aujourd'hui n'est pas adapté à la problématique des réseaux interdépendants.

3.1 Cahier des charges

Le SAP appliqué aux réseaux interdépendants doit répondre à un certain nombre de besoins spécifiés par les demandeurs (opérateurs des réseaux et responsables de la sécurité civile) lors du lancement du projet :

- Le système doit présenter clairement et sous une interface visuelle conviviale la propagation dans l'espace et dans le temps d'une défaillance au sein de réseaux interdépendants,
- La visualisation de la propagation dans l'espace doit fournir aux exploitants de réseaux de l'information géographique leur permettant de localiser la défaillance et ses conséquences. Cette information sera nécessaire à la mise en œuvre de mesures de gestion appliquée à un secteur géographique limité et clairement identifié. Ce secteur géographique sera susceptible d'évoluer au fil du temps en fonction de la propagation de la défaillance,
- La visualisation de la propagation dans le temps doit fournir aux exploitants de réseaux un préavis leur permettant d'anticiper les conséquences de la défaillance sur leur propre réseau ainsi que sur les réseaux auquel ils seront interconnectés. Cette information autorisera la mise en œuvre de mesures de gestion planifiées et adaptées selon les délais indiqués par le système,
- Une fois validées dans leur forme ainsi que dans leur contenu, ces informations de propagation dans l'espace et dans le temps seront agrégées au sein d'un message d'alerte dont la diffusion amènera la mise en œuvre par les différents réseaux de mesures de gestion appropriées,

3.2 Définition et composantes d'un SAP

Comme illustré dans la revue de littérature, il n'existe ni définition, ni forme universelle de SAP, ainsi, nous allons devoir définir ces 2 aspects pour qu'ils soient adaptés à notre problématique de recherche.

3.2.1 Définition

L'intérêt d'étendre les fonctions du système expert par la mise en place d'un SAP est que ce dernier va permettre de mieux faire face aux conséquences des défaillances. Ce doit donc être un outil convivial, mais aussi précis et rigoureux.

Lorsque les exploitants de réseau font face à une défaillance, le seul moyen dont ils disposent pour en limiter les conséquences est de ne pas rester sans rien faire, sans quoi la défaillance va continuer à se propager librement dans le temps et dans l'espace au-delà même des limites du système. Aussi, il va être nécessaire pour eux de disposer d'un certain nombre d'éléments d'appréciation leur permettant de prendre des décisions de gestion appropriées.

Dans ce contexte, la définition donnée ici d'un SAP est qu'il s'agit d'un outil fournissant de l'information opportune et pertinente sur la survenue d'une défaillance, dès lors que cette information permet de prendre des mesures de gestion en limitant les conséquences.

3.2.2 Composantes

La composition d'un SAP n'est pas universelle et elle doit être pensée en fonction de l'environnement dans lequel il est destiné à être implanté. Il a été ainsi nécessaire de définir un certain nombre de composantes du SAP selon la définition de l'outil, ses objectifs et le cahier des charges des partenaires.

L'article en annexe présente et détaille les 6 composantes qui ont été considérées indispensables au développement d'un SAP en général, ainsi que les caractéristiques de l'information qui doit être présente dans chacune de ces composantes. Appliqué à la problématique des réseaux interdépendants, le contenu de ces 6 composantes se décline de la façon suivante :

1. L'outil

L'outil en lui-même peut revêtir plusieurs formes. Partant du principe que le SAP est une extension de *Domino*, et que *Domino* dispose déjà d'un outil de visualisation, il est apparu intéressant d'utiliser une interface si ce n'est identique, au moins facile à connecter aux informations du système expert.

2. La connaissance du système et l'identification des situations dangereuses

Pour fonctionner efficacement, le SAP doit prendre en compte les caractéristiques du milieu dans lequel il est implanté. *Domino* dispose de ces données qui seront prises en compte dans les visualisations du SAP.

3. Le choix des indicateurs et de l'information présentée

Le choix des indicateurs sera fonction de 2 critères :

- Les paramètres disponibles dans *Domino*, puisque le système expert centralise l'information relative aux interdépendances,
- Le cahier des charges défini avec les utilisateurs et qui spécifiera leurs besoins.

Dans tous les cas, l'information efficace devra être :

- Opportune, c'est-à-dire qu'elle doit être délivrée en un temps donné afin d'indiquer aux intervenants de quel délai ou quelle marge de manœuvre ils disposent.
- Pertinente, c'est-à-dire ciblée. Trop d'indicateurs et l'outil devient soit illisible (comme un tableau de bord avec trop de cadrans), soit imprécis (l'information pertinente sera noyée dans de l'information inutile). À l'inverse, si trop peu d'indicateurs sont disponibles, l'outil ne remplit pas efficacement sa fonction.

4. L'identification des délais

Aucune mesure de gestion efficace ne peut être mise en place sans considération du délai des perturbations. Les indicateurs présentés devront être lus sur une échelle de temps afin de fournir aux opérateurs une capacité d'anticipation sur les conséquences de la défaillance, capacité se traduisant par la mise en place de mesures de gestion non seulement au sein de leur propre réseau, mais également dans les réseaux avec lesquels ils seraient interdépendants.

5. L'alerte

L'un des buts principaux du SAP est de transmettre une alerte, chaque seuil d'alerte devant générer une action et mobiliser les ressources correspondantes. Lors de sa conception, il est donc nécessaire de définir :

- Les modalités de déclenchement de l'alerte : au sein du système concerné, il faudra identifier la structure, le niveau hiérarchique adapté et l'individu chargé du déclenchement de l'alerte, à partir des éléments d'appréciation – notamment l'identification de seuils - fournis par le SAP.
- Les caractéristiques de l'alerte qui sera transmise : une alerte unique ou à l'inverse une alerte à plusieurs niveaux, ou de type différent selon différents destinataires,
- Le moyen de transmission : selon le système étudié, plusieurs supports seront envisageables, du plus simple au plus complexe. Ce moyen peut être nouveau, ou bien déjà existant auquel une fonction d'alerte précoce sera intégrée.
- Les destinataires concernés, qui sont de 2 types :
 - o les intervenants intéressés : il s'agira des opérateurs des IE partenaires, ainsi que des bureaux de sécurité civile,
 - o le public : à partir des informations fournies par le SAP, l'alerte devra cibler géographiquement et dans le temps le public concerné et leur proposer de l'information et des conduites à tenir. La prise en charge de cette fonction revient naturellement aux bureaux de sécurité civile.

6. Les mesures de gestion

Le SAP n'a d'intérêt que si l'information qu'il fournit permet de prendre des mesures destinées à limiter les conséquences d'une défaillance. La mise en place d'un tel outil doit donc s'accompagner de la mise en place simultanée de mesures de gestion adaptées à la défaillance considérée. Ces mesures de gestion doivent couvrir les aspects d'intervention (afin de limiter les conséquences de la défaillance) avec notamment la mise en œuvre des RA adaptées, et d'information (des intervenants privés ou publics concernés et de la population). Elles seront par nature transversales aux différents réseaux étudiés puisqu'elles amèneront un changement d'état de l'un qui aura une influence directe sur l'état des autres avec lequel il est interconnecté.

3.2.3 La maîtrise des composantes

Lorsqu'il s'est agit de comprendre les difficultés de mise en place de la maquette de SAP à Montréal, il a fallu notamment reconsidérer les informations disponibles pour chacune de ses composantes développées plus haut.

L'article en annexe détaille l'étude de ces informations pour 2 SAP, le *Homeland Security Advisory System* (HSAS) et le système d'alerte de l'Organisation Mondiale de la Santé (OMS) en cas de pandémie grippale. En effet, après un temps plus ou moins long d'utilisation, ces 2 systèmes ont été modifiés ou remplacés par leurs administrateurs parce qu'ils ne répondaient pas aux besoins. Lorsque l'on étudie les informations disponibles pour chacune des composantes de ces systèmes, on ne peut que constater que certaines informations indispensables, n'ont, soit pas du tout été intégrées aux systèmes, soit n'ont pas le niveau de détail nécessaire pour être pertinentes. Des constatations identiques ont été établies lors de l'étude, à partir d'un tableau similaire, des difficultés d'implantation de notre propre système.

Ces observations montrent que la maîtrise des composantes d'un SAP, c'est-à-dire l'intégration des informations pertinentes dans chacune de ses différentes composantes, est un élément crucial de l'adéquation du système à l'environnement pour lequel il a été conçu.

3.3 Paramètres retenus pour les visualisations

La composante de choix des indicateurs et de l'information présentée amène à rechercher les paramètres disponibles à l'alimentation en données du SAP. Deux types de paramètres ont été identifiés et intégrés aux visualisations. Il s'agit d'une part d'indicateurs relatifs à la propagation de la défaillance, et d'autre part d'indicateurs relatifs aux effets de la défaillance sur le système.

3.3.1 Indicateurs relatifs à la propagation de la défaillance

Ces indicateurs sont fournis par le système expert. Il s'agit :

- De la ressource,
- De l'état de la ressource,
- Du secteur en cause,

- Des délais entre les différents états de la ressource.

Un indicateur relatif au réseau en cause était également disponible mais n'a pas été retenu. En effet, un réseau peut supporter plusieurs ressources, par exemple le réseau de télécommunications supportant les ressources *Voix* et *Données*, et il a paru plus précis de se concentrer sur l'état de chacune des ressources plutôt que sur celui du réseau qui les supporte. Néanmoins, une visualisation par réseau en cause est toujours possible.

3.3.2 Indicateurs relatifs aux effets de la défaillance sur les ressources

Ces indicateurs proviennent de l'étude des différents modes de propagation d'une défaillance qui permet de mettre en évidence 5 types d'effets sur les ressources et les réseaux.

- *Effets sur les réseaux interdépendants*

L'interruption initiale d'une ressource a un effet direct sur d'autres réseaux avec lesquels le réseau initial a une interdépendance fonctionnelle.

- *Effets sur les réseaux dépendants*

L'interruption initiale d'une ressource a un effet sur d'autres réseaux ayant besoin de cette ressource pour fonctionner, ces réseaux n'ayant pas d'interdépendance fonctionnelle avec le premier.

- *Effets domino*

L'interruption initiale d'une ressource a un effet sur un autre réseau qui a lui-même une interdépendance avec un troisième réseau. La dégradation du service du troisième réseau n'a qu'un lien indirect avec la panne initiale.

- *Effets rebond*

Les cascades d'effets successifs ont finalement de nouveau un impact sur le réseau source de l'interruption initiale.

- *Effets cumulatifs*

Sans gestion efficace, la dégradation continuera à se propager au sein des réseaux dépendants et interdépendants, les uns affectant et se retrouvant affectés par les autres. Les effets cumulatifs

rassemblent l'ensemble des effets précédents et seront susceptibles de se propager au sein des réseaux interdépendants selon un schéma difficile à prédire compte tenu du nombre de réseaux affectés et de la complexité de leurs interconnexions.

3.4 Visualisations obtenues

Plusieurs types de visualisations ont été obtenus en combinant les différents paramètres à disposition.

3.4.1 Visualisations par indicateurs relatifs à la propagation de la défaillance

Quatre indicateurs sont disponibles pour ces visualisations. Ceux-ci peuvent être combinés de 4 manières différentes, chacune fournissant de l'information selon un angle particulier. Comme évoqué plus haut, les RA ne sont pas prises en compte dans ce premier volet de visualisations, ainsi la ressource ne peut avoir que 2 types d'état, soit disponible (vert), soit indisponible (rouge). La numérotation des secteurs est celle utilisée au CRP (figure 2.2).

L'hypothèse de départ était une interruption de la fourniture d'eau dans le secteur AH-21. Les conséquences illustrées ne reflètent pas ici la réalité des interdépendances des réseaux sur l'île de Montréal, ce ne sont que des cas d'étude retenus pour illustrer les différentes visualisations retenues.

1. Visualisation par ressource

La figure 3-1 illustre une visualisation par ressource pour les télécommunications. En abscisse du graphique on retrouve le délai alors qu'en ordonnée, les secteurs en cause sélectionnés selon les zones d'alimentation des réseaux. Les couleurs indiquent l'état de la ressource comme indiqué ci-dessus. Nous voyons dans cet exemple que la panne initiale provoque une interruption des télécommunications *Voix* dans les secteurs AG-22 et AH-22 à partir de la troisième heure.

Cette visualisation est utile pour l'exploitant de l'infrastructure de télécommunication : elle lui indique que la ressource *Voix* de son réseau va subir les conséquences de l'interruption d'eau initiale après un délai de 2 heures et dans 2 secteurs de son réseau de distribution, et lui permet de mettre en œuvre les mesures de gestion internes destinées à en limiter les conséquences.

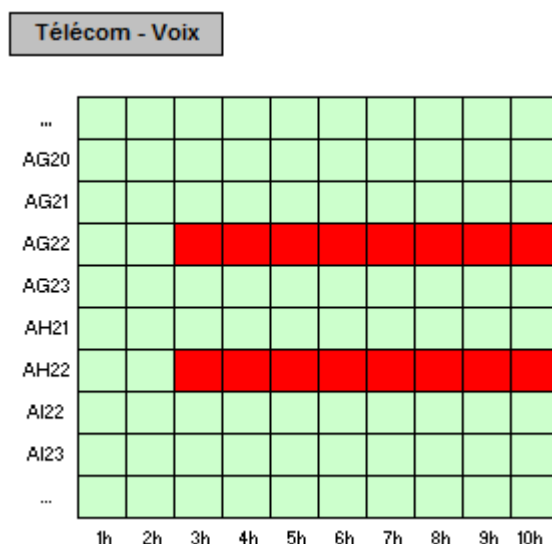


Figure 3.1 : Exemple de visualisation par ressource

2. Visualisation par état

La figure 3.2 illustre la visualisation de l'état d'indisponibilité des ressources dans l'exemple considéré. La panne initiale (eau en AH-21) est mentionnée ainsi que ses effets (interruption eau et télécom en AH-22, et télécom et transports en AG-22 à partir de la 3^{ème} heure).

Cette visualisation est utile pour les exploitants de réseaux ainsi que pour la Sécurité civile. D'une part, elle synthétise pour les exploitants les interruptions des différentes ressources dans les différents secteurs selon une échelle de temps, permettant de prendre des mesures transversales de gestion des différentes pannes. D'autre part, elle permet à la Sécurité Civile de connaître les défaillances à venir afin de prendre des mesures visant à protéger la santé et la sécurité des populations des secteurs considérés.

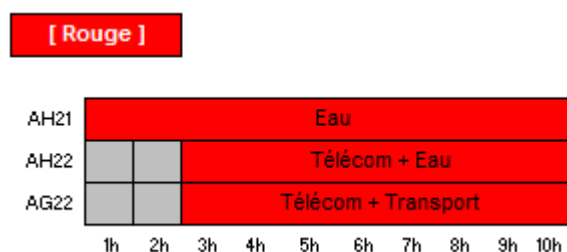


Figure 3.2 : Exemple d'une visualisation par état

3. Visualisation par secteur

La figure 3.3 illustre les défaillances constatées pour le secteur AH-22. On y constate une interruption des télécoms à partir de la 3^{ème} heure, ainsi que de l'électricité à la 7^{ème} heure et de l'eau à la 8^{ème}.

Cette visualisation est utile pour la Sécurité civile. En ciblant un secteur en particulier, elle lui permet de prendre des mesures géographiquement adaptées en fonction des défaillances des différentes ressources.

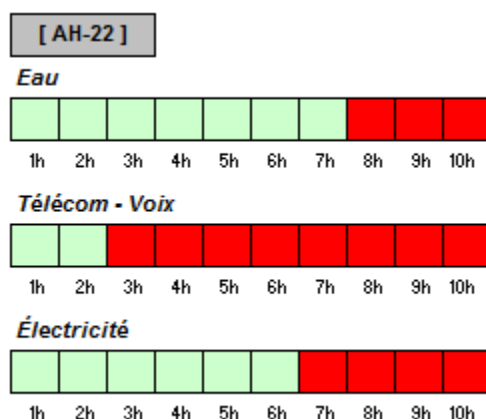


Figure 3.3 : Exemple d'une visualisation par secteur

4. Visualisation par délai

La figure 3.4 illustre l'état de disponibilité des ressources à la 7^{ème} heure. On constate une interruption d'eau en AH-21 (la panne initiale), des télécoms en AG-22 et AH-22, de l'électricité en AH-22 et des transports en AG-22.

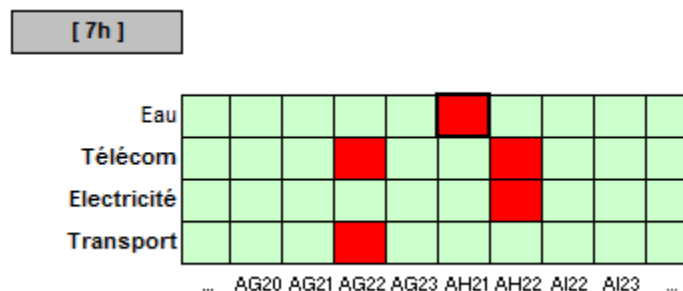


Figure 3.4 : Exemple de visualisation par délai

Cette visualisation est également utile pour les exploitants de réseaux et la Sécurité civile. En mettant en évidence les défaillances de certaines ressources dans certains secteurs, elle fournit à ces 2 acteurs le préavis nécessaire à la mise en place des mesures de gestion adaptées, en particulier en ce qui concerne le choix et la mise en œuvre des RA.

3.4.2 Visualisations par indicateurs d'effets

Les 5 effets identifiés plus haut peuvent aussi faire l'objet de visualisations.

1. Effet sur les réseaux interdépendants

La figure 3.5 illustre les effets de la panne initiale sur les réseaux interdépendants avec deux niveaux de précision.

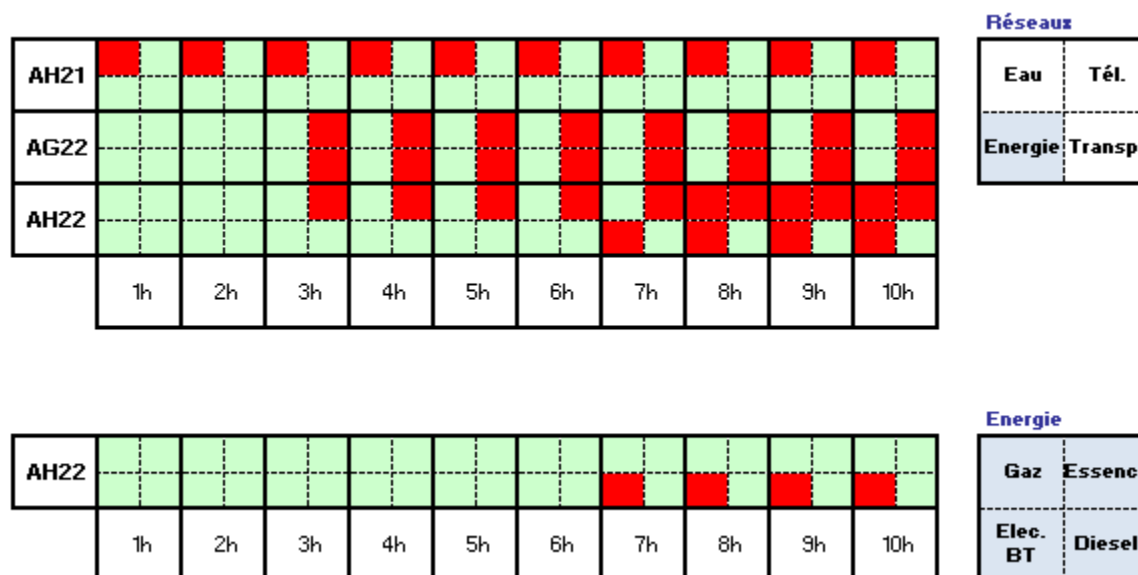


Figure 3.5 : Visualisation d'effet sur les réseaux interdépendant

Dans le tableau du haut, 4 réseaux (eau, télécom, transport et énergie) sont illustrés dans chaque carré secteur/délai. Dans le tableau du bas, le réseau énergie a été subdivisé en 4 ressources (gaz, essence, électricité basse tension et diesel).

Les codes couleur utilisés sont les mêmes que précédemment. On voit par exemple que pour le secteur AH-22 à la 7^{ème} heure, les réseaux *énergie* et *télécom* sont défaillants (tableau du haut), et en particulier pour le réseau *énergie* l'électricité basse tension (tableau du bas).

Cette visualisation est particulièrement favorable à la mise en place de mesures de gestion transversales. En effet, elle synthétise dans les secteurs géographiques concernés et sur une échelle de temps la dégradation de plusieurs ressources sur un seul tableau de bord, et selon 2 niveaux de précision, les réseaux en eux-mêmes, ou chacune des ressources supportées par les différents réseaux.

2. Effets sur les réseaux dépendants

La visualisation pour les réseaux dépendants est la même que dans la figure 3.5 ci-dessus en intégrant dans le cartouche *Réseaux* les réseaux dépendants au lieu des réseaux interdépendants.

Comme dans le cas précédent, cette visualisation aide à la mise en place de mesures de gestion transversales.

3. Effets domino

La figure 3.6 illustre la visualisation d'un effet domino de la panne initiale d'eau en AH-21 sur les réseaux *télécom* et *transport* en AG-22. Seuls ces deux derniers réseaux sont retenus dans la matrice puisqu'ils sont les seuls dans l'exemple à subir un effet domino.

Eau	AH-21										
Télécom	AG-22										
Transport	AG-22										
		1h	2h	3h	4h	5h	6h	7h	8h	9h	10h

Figure 3.6 : Exemple de visualisation d'effet domino

Cette visualisation est particulièrement utile à l'exploitant du réseau de la panne initiale et à celui du réseau qui subit l'effet domino. En effet, il n'y a pas de lien évident entre eux à première vue, aucun n'utilisant la ressource de l'autre. Pourtant, la présence d'un réseau intermédiaire relayant la défaillance initiale va créer une relation de cause à effet entre ces 2 réseaux. Les exploitants de chacun de ces réseaux seront avertis de la propagation d'une défaillance de l'un vers l'autre.

4. Effet rebond

La figure 3.7 illustre un effet rebond. La panne initiale d'eau en AH-21 va générer une nouvelle panne d'eau à partir de la 8^{ème} heure dans le secteur AH-22.

Cette visualisation est particulièrement utile à l'exploitant de la ressource initiale dans la mesure où elle va le prévenir d'une aggravation de l'état de sa ressource sur d'autres secteurs que celui de la panne initiale et lui fournira le préavis nécessaire à la mise en œuvre des mesures de gestion adaptées.

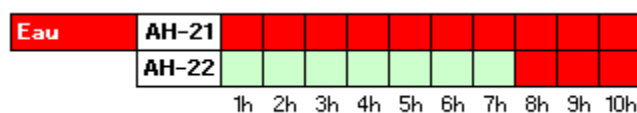


Figure 3.7 : Exemple de visualisation d'effet rebond

5. Effets cumulatifs

La figure 3.8 illustre un exemple d'effets cumulatifs à un niveau plus large (secteur centre-ville de Montréal). Elle indique quels types d'interdépendances (fonctionnelle ou géographique) vont avoir les réseaux dépendants et interdépendants (en abscisse) avec les réseaux à l'étude (en ordonnée), permettant ainsi d'anticiper sur l'évolution de l'état de chacun d'entre eux selon l'état des autres.

De par la visualisation synthétique qu'elle propose, elle est un outil d'aide à la décision quant aux mesures à prendre non seulement pour les exploitants de réseaux dépendants et interdépendants et la Sécurité civile, mais également pour d'autres acteurs primordiaux tels que les services gouvernementaux du niveau local au niveau national, selon le schéma de propagation des défaillances.

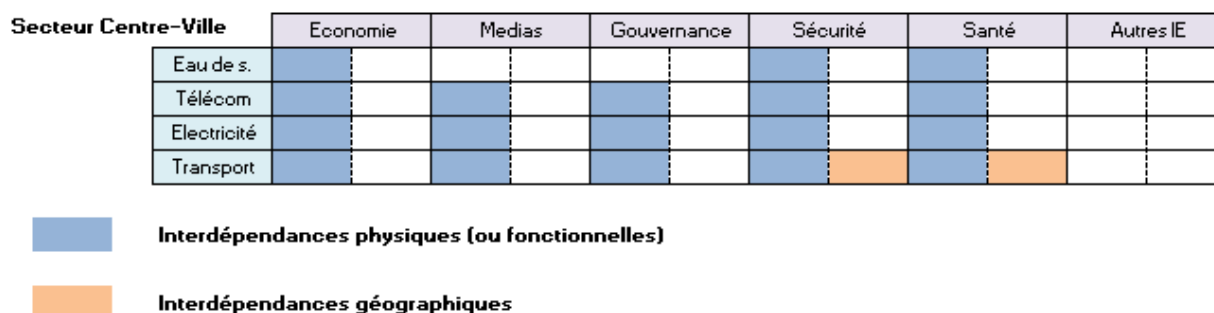


Figure 3.8 : Exemple de visualisation d'effets cumulatifs

3.5 Prise en compte des RA

Ces différentes visualisations peuvent être améliorées en intégrant les RA adaptées. En effet, les exploitants de réseaux disposent généralement de RA capables de pallier la défaillance d'une ressource initiale. Ainsi, dans la réalité, l'état du réseau ne passe pas directement du stade *disponible* au stade *indisponible* mais passe par une phase *disponible grâce à une ressource alternative* que nous allons illustrer ici.

3.5.1 Indicateurs de niveau de fonctionnement

Les différents états du réseau selon l'utilisation d'une RA seront illustrés par l'indicateur du niveau de fonctionnement d'un réseau (tableau 2.1), avec les modifications suivantes :

Vert	Le réseau fonctionne normalement avec les ressources qu'il utilise couramment.
Jaune	Le réseau fonctionne grâce à la mise en place d'une ressource alternative <u>autonome</u> .
Orange	Le réseau fonctionne grâce à la mise en place d'une ressource alternative <u>dépendante</u> .
Rouge	Le fonctionnement du réseau est compromis, la ressource fournie n'est pas disponible.

Tableau 3.1 : Niveaux de fonctionnement avec ressource alternative

3.5.2 Caractérisation des RA

Chaque RA peut se caractériser au travers de 4 paramètres, 2 liés au délai de sa mise en œuvre et 2 liés à sa propre dépendance à une autre ressource. L'état de fonctionnement du réseau prendra en compte les caractéristiques de disponibilité de la ressource alors que son temps de mise en œuvre indiquera à l'exploitant de réseau sous quel délai minimal il peut compter sur la ressource alternative et prendre des mesures de gestion en conséquence.

1. Caractéristiques de délai

La RA **immédiatement disponible** supplée immédiatement à la défaillance de la ressource courante, alors que la RA **disponible avec délai** est caractérisée par un temps de mise en œuvre variable en fonction d'autres facteurs (acheminement, temps d'alimentation et de mise en route, disponibilité des opérateurs, ...). La figure 3.9 illustre ces 2 états : la batterie est immédiatement

disponible et fonctionnera selon son autonomie prévue, alors que la génératrice aura besoin d'un temps de mise en œuvre avant de fonctionner.

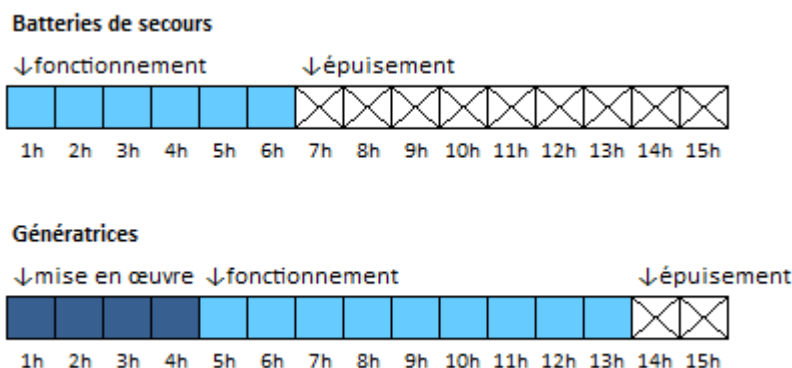


Figure 3.9 : Caractérisation d'une RA

2. Caractéristiques de dépendance

La RA peut être soit **autonome**, c'est-à-dire qu'elle fonctionne jusqu'à épuisement sans autre ressource extérieure, ou **dépendante** d'une ressource extérieure. La figure 3.9 illustre également la durée de fonctionnement de la génératrice qui est variable et dépendante d'une autre ressource, le carburant pour l'alimenter.

3. Courbe de dépendance d'une RA

Les paramètres de caractérisation d'une RA nous suggèrent qu'il est possible de développer des courbes de dépendance aux ressources alternatives. En effet, l'utilisation d'une RA immédiatement disponible et autonome ou à l'inverse nécessitant un long délai de mise en œuvre et une forte dépendance à une autre ressource va amener à des procédures de gestion totalement différentes où il faudra prendre en compte, dans le 2^{ème} cas, des contingences à type de disponibilité de la RA elle-même et de ses dépendances, ainsi que d'acheminement et de modalités de mise en œuvre.

La figure 3.10 illustre cet état de fait. La génératrice 1 nécessite une durée significative avant de pouvoir être utilisée (6h) et ne dispose que d'un temps de fonctionnement relativement bref (5h), alors que la génératrice 2 est mise en œuvre très rapidement (1h) et dispose d'une très grande autonomie (>15h). La connaissance de ces caractéristiques est fondamentale pour les exploitants

de réseaux lorsqu'il s'agira pour eux de décider des ressources alternatives à identifier ou à mettre en œuvre.

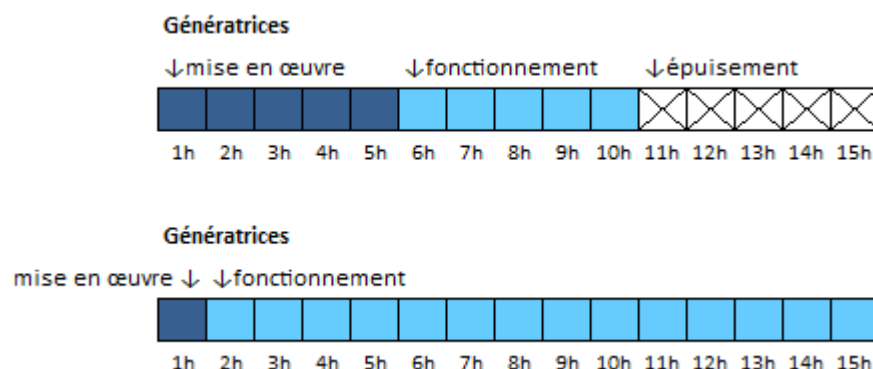


Figure 3.10 : Dépendance à une RA

3.5.3 Intégration des RA dans les visualisations

Il est maintenant possible d'intégrer les RA dans les visualisations initiales afin de donner une idée plus réaliste des différents états du réseau, qui ne sera plus simplement *disponible* ou *indisponible*, mais sera fonction des RA à disposition.

1. Modalités d'intégration

L'intégration d'une RA va modifier le graphique de défaillance initial, en rendant fonctionnel la ressource initiale durant la durée de disponibilité de la ressource alternative. Dans la figure 3.11, l'eau en citerne permet de pallier la panne d'eau initiale à partir de la 5^{ème} heure (après son délai de mise en œuvre) et jusqu'à la 14^{ème} heure (selon son autonomie). Ainsi l'eau avec RA redevient disponible entre la 5^{ème} et la 14^{ème} heure, illustré par la couleur orange de dépendance à une RA elle-même dépendante (tableau 3.1).

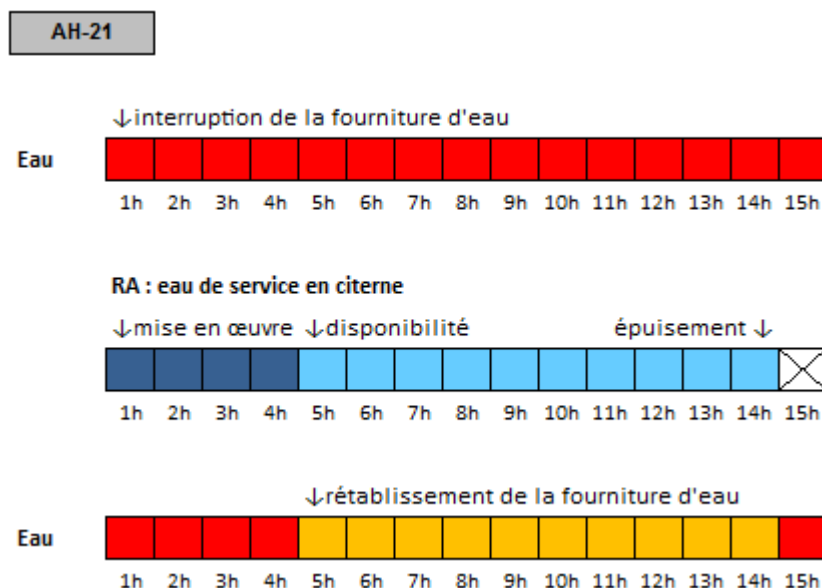


Figure 3.11 : Exemple d'intégration d'une ressource alternative

2. Exemple de résultats

En combinant les différentes RA aux différents réseaux, il est possible d'obtenir une synthèse des visualisations pour un secteur donné.

Dans la figure 3.12, on applique 3 ressources alternatives (batteries, génératrices et eau en citerne) à 3 ressources défaillantes (électricité, télécom et eau) en AH-22.

Le premier graphique montre les effets de l'interruption d'eau initiale en AH-21 sur les ressources électricité, télécoms et eau dans le secteur AH-22. Sans l'utilisation de RA, ces ressources deviennent défaillantes respectivement à la 7^{ème}, 3^{ème} et 8^{ème} heure.

Le second graphique indique que 3 RA sont disponibles pour faire face à ces défaillances : des batteries de secours, des génératrices et de l'eau de service en citerne. Chacune de ces RA dispose de sa propre courbe de dépendance. Les batteries de secours fonctionneront instantanément pour une durée de 6 heures, les génératrices seront en fonction de la 5^{ème} à la 14^{ème} heure – cette durée dépendant de la capacité d'alimenter les génératrices en carburant -, et le volume d'eau en citerne disponible permettra d'alimenter les réseaux pour 10 heures à partir de la 5^{ème} heure.

Le troisième graphique, en bas de figure, montre qu'ainsi les ressources sont maintenues fonctionnelles grâce à l'emploi judicieux des RA, jusqu'à la 15^{ème} heure pour les télécoms et bien au-delà pour les autres ressources, soit par l'intermédiaire des RA autonomes (batteries, courbes en jaune) ou dépendantes à une autre ressource (génératrices et eau de service, courbes en orange).

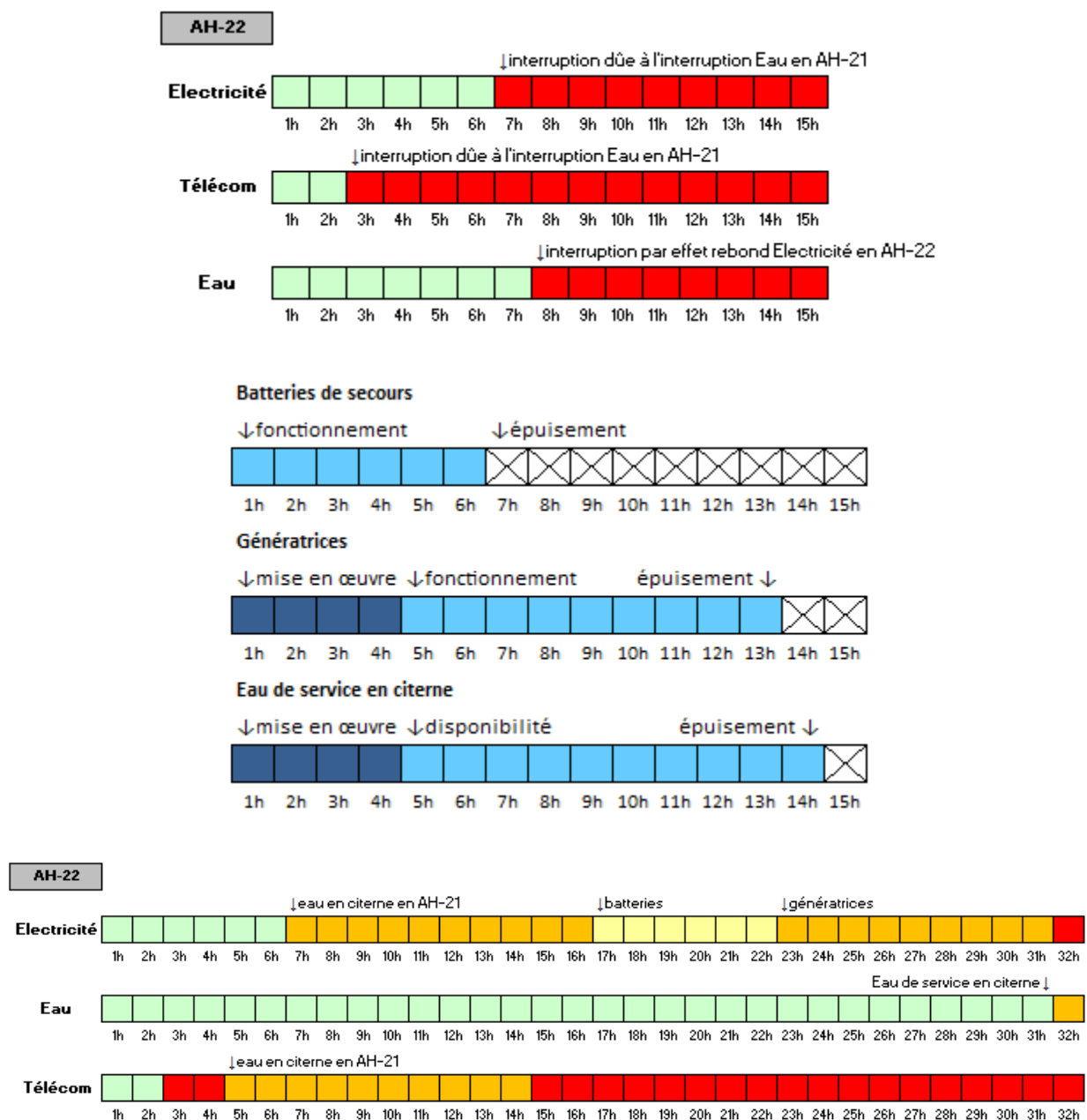


Figure 3.12 : Exemple de résultats

3.6 Synthèse des résultats

La maquette de SAP a été présentée pour avis et commentaires, à différentes phases de son développement, aux exploitants des réseaux partenaires ainsi qu'à la Sécurité civile de Montréal lors de plusieurs réunions communes. La dernière réunion est celle qui a soulevé le plus d'objections quant à l'outil et à l'idée même d'implanter un SAP au sein de réseaux interdépendants.

Ces divergences ont amené à reconsidérer le SAP dans son ensemble, l'outil et le concept, et ont permis d'identifier un certain nombre de paradoxes propres à empêcher dans le contexte actuel son évaluation puis son opérationnalisation.

Cette analyse et les conclusions auxquelles elle aboutit sont présentées dans l'article en annexe.

CHAPITRE 4 DISCUSSION GÉNÉRALE

Les travaux menés lors de ce projet de recherche ont permis d'améliorer les connaissances du CRP sur les SAP et à la fois d'en donner une définition, d'en définir un ensemble de composantes ainsi qu'une maquette d'application pratique appliqués à notre environnement de travail.

Or, comme il l'a été souligné précédemment, le développement du SAP au sein des réseaux interdépendants n'a pas pu être mené jusqu'à son terme et son implantation n'a pas pu être testée. En effet, après quelques mois de développement, les partenaires ont émis plusieurs objections, non seulement sur la maquette elle-même, mais également sur l'intérêt global d'un SAP. Cette position assez inattendue nous a poussés à reconsidérer notre système dans son ensemble et à nous interroger sur les racines des difficultés à le mettre en place.

Des difficultés organisationnelles ...

Dans un premier temps, nous avons reconsidéré notre système en fonction des caractéristiques intrinsèques d'un SAP et avons pu ainsi déterminer que l'environnement de développement n'était aujourd'hui pas propice à la mise en place d'un tel système, parce que cet environnement ne met pas à disposition les informations nécessaires à ce que le SAP fournisse de l'information pertinente et opportune. En effet, lorsque que l'on recherche dans notre système les paramètres qui s'appliquent à chacune des composantes du SAP telles que nous les avons définies, force est de constater que certains éléments fondamentaux manquent alors que d'autres restent imprécis. Par exemple, la connaissance du système et des défaillances est insuffisante car la précision des données d'appréciation sont limitées par les exploitants de réseaux. Les données à disposition ne permettent pas non plus de déterminer de seuils d'alerte fiables devant mener à la mise en place de mesures de gestion, ni de déterminer quelles mesures de gestion mettre en place, non seulement par chacun des réseaux, mais également de manière transversale, entre réseaux. Enfin, bien que l'espace de coopération soit une réalité, aucune position commune n'a pu être trouvée quant aux modalités de déclenchement des alertes.

Dans un deuxième temps, nous avons reconsidéré le système du point de vue des exploitants et avons pu mettre en évidence 2 paradoxes qui expliquent les réticences à son implantation.

Le premier paradoxe est que, bien que l'ensemble des partenaires reconnaisse que le développement d'un SAP fait partie intégrante du projet 2008-2012 du CRP, aucun aujourd'hui ne souhaite se lancer plus avant dans la démarche pour un certain nombre de raisons liées à la fois au SAP en lui-même mais également au système expert qui le supporte. En effet, lorsque le sujet de l'opérationnalisation du système expert a été abordé, c'est-à-dire son transfert du CRP à un autre organisme qui prendrait en charge son suivi et son fonctionnement ou à l'inverse le financement du CRP pour qu'il puisse mettre les ressources nécessaires à le faire, la question de la pérennité de l'outil s'est immédiatement posée. D'une part, le maintien en fonction du système expert va nécessiter des ressources et de l'expertise qui aujourd'hui sont centralisées au CRP, alors que, demain, la gestion de l'outil pourrait être confiée à une autre structure. D'autre part, il sera nécessaire de régulièrement actualiser les données du système selon les modifications de chacun des réseaux, voire d'introduire de nouveaux paramètres si de nouveaux réseaux se joignent à l'étude. Dans ce contexte, le système expert est destiné à grossir et à se complexifier, et ainsi à demander un niveau de ressources techniques et financières grandissant, ce qui se révèle être un point bloquant pour les partenaires. Aussi, si le système expert n'est pas amené à se développer à cause de ces contraintes, les partenaires s'interrogent sur l'intérêt de développer un SAP qui s'y rattache.

Un deuxième aspect lié au système a soulevé des objections, celui des procédures de gestion. Les exploitants de réseaux disposent aujourd'hui de leurs procédures internes de gestion des défaillances. De son côté, le SAP met en évidence la nécessité de mesures de gestion transversales, notamment lorsqu'il s'agit de la mise en œuvre de RA communes, puisque par définition la quantité et la disponibilité de telles ressources sont limitées. Par exemple, les besoins en RA indiqués par les exploitants de réseau ont permis de mettre en évidence que le volume de carburant nécessaire à l'alimentation de leurs génératrices poserait rapidement un problème en cas de panne prolongée d'électricité (Robert & Morabito, 2009a).

Ainsi, partant du constat que tous les réseaux ne pourront pas disposer de toutes les ressources alternatives dans tous les secteurs et dans n'importe quelles quantités, il devient évident qu'il va falloir définir des priorités de gestion. Ces priorités reposeront à la fois sur la criticité d'alimentation en RA (on comprend par exemple qu'un hôpital est sans doute prioritaire lorsqu'on évoque la fourniture d'eau ou d'électricité), sachant que les priorités d'alimentation seront décidées par le pouvoir politique et pas par les exploitants de réseaux, et sur la quantité

disponible de la RA en question selon les différents secteurs géographiques. Non seulement pour les réseaux qui bénéficieront des RA en quantité limitée et sous un délai plus ou moins long de mise en œuvre, mais également pour les autres réseaux qui devront, eux, se passer de RA et définir d'autres modes de gestion, on comprend qu'il sera nécessaire de développer des mesures de gestion inter-réseaux prenant en compte la disponibilité en quantité et en délai des RA. Or, les exploitants ne voient pas aujourd'hui comment mettre en place ces procédures, ni comment les articuler avec les procédures internes à chacun des réseaux.

Le deuxième paradoxe est lié à l'écart entre les attentes des exploitants de réseau quant à la précision du système et le niveau de détail des informations qu'ils sont prêts à partager. Pour des raisons de confidentialité, l'espace de coopération a décidé, dès le début des projets, de travailler sur la base d'une cartographie souple dans laquelle les infrastructures seraient positionnées au sein de carrés de 1km de côté avec un degré de précision variable selon les choix des réseaux. Cette demande provenait explicitement des exploitants qui, pour des raisons de confidentialité, étaient plus ou moins réticents à partager l'emplacement précis de leurs infrastructures. Cette relative imprécision se retrouve dans les informations fournies par le SAP : à partir des informations à disposition, le système n'est capable de localiser les dégradations qu'avec la précision qui lui est imposée, en l'occurrence 1km², alors que les exploitants souhaiteraient avoir une information sur la position de la défaillance d'un niveau de précision égal à celui qu'ils ont de leurs propres cartographies des zones d'alimentation, ce qui est incompatible.

Plusieurs pistes sont envisageables pour faire face à ces difficultés et tenter à l'avenir une nouvelle implantation du système :

- Les seuls commentaires concernant l'outil SAP en lui-même est qu'en tant qu'extension de *Domino*, le fonctionnement du premier est directement lié à la pérennité du second. Ainsi, si le CRP et ses partenaires parviennent à un accord sur l'avenir de *Domino*, en particulier ses modalités de portage et de financement, le SAP pourra naturellement s'y ajouter.
- La connaissance du système et des situations dangereuses, ainsi que la qualité des informations présentées par le SAP sont directement liés à la précision des informations fournies par les exploitants de réseau. Plus les données d'entrée sont détaillées, plus le résultat fourni par le SAP est précis. Il serait nécessaire d'interroger les exploitants de

réseau sur le niveau de détail technique et géographique qu'ils souhaitent, et, en fonction, de leur indiquer de quel niveau de détail des données d'entrée *Domino* aura besoin afin que le SAP puisse fournir le résultat attendu. La confidentialité des données de chaque réseau sera le principal obstacle à l'obtention de ce niveau de détail. Cette difficulté pourrait être contournée par, à la fois, un accord formel des différentes directions des réseaux à partager un certain type et niveau de données, la signature d'un accord de confidentialité liant les participants à l'espace de coopération, et une procédure de sécurisation, de gestion et de partage des informations identifiées comme confidentielles.

- L'efficacité de la transmission de l'alerte est liée au fait que chaque réseau dispose de sa propre chaîne d'alerte interne et qu'il n'a pas été possible d'identifier, pour le SAP, quel organisme et quel niveau hiérarchique devrait déclencher l'alerte initiale. Cette difficulté a un lien direct avec le portage du système expert. En phase opérationnelle, le système doit idéalement pouvoir être interrogé dès la panne initiale, quelque soit le jour ou l'heure, afin de disposer du préavis maximal pour la mise en œuvre des mesures de gestion appropriées. L'alerte, en conséquence, devrait pouvoir être déclenchée dans les mêmes conditions, ce qui signifie que le système devrait être porté dans son ensemble par un organisme fonctionnant 24h/24 et 7j/7, capable de réagir instantanément dès la détection d'une défaillance initiale.
- En ce qui concerne les mesures de gestion, il serait nécessaire, dans un premier temps, que l'ensemble des membres de l'espace de coopération reconnaisse la nécessité de mesures de gestion transversales, afin qu'ensuite des groupes de travail partageant leurs procédures internes afin de définir des procédures inter-réseaux puissent être constitués. Dans cette optique, il pourra être intéressant de travailler ressource par ressource et de n'inviter dans ces groupes que les exploitants de réseaux concernés par les défaillances, selon les modélisations de *Domino*. Les procédures transversales n'en seraient que plus pertinentes, puisque plus ciblées sur une problématique limitée. Gardant à l'esprit que la propagation d'une défaillance est limitée grâce à la mise en œuvre de mesures de gestion adaptées, ces procédures seraient essentiellement destinées à proposer des conduites à tenir.

En l'état actuel des choses, nous constatons donc, d'une part, l'inadéquation du SAP à l'environnement dans lequel il est sensé être implanté dans l'état actuel du niveau de précision des données fournies, et, d'autre part, que la mise en œuvre des pistes de solution proposées s'étalera sur une période de temps difficile à prévoir. Aussi, afin de capitaliser sur le travail effectué et ses pistes d'amélioration, il serait intéressant de repenser l'alerte précoce, non pas en tant qu'outil mais plutôt en tant que concept et d'étudier en détail ce que recouvre le terme afin d'adapter l'outil à d'autres utilisations au sein d'un concept global d'alerte précoce qui pourrait recouvrir des aspects relativement larges liées à la planification, tels que la mise en place d'exercice qui permettraient la validation de mesures de gestion adaptées aux défaillances modélisées par *Domino*, la définition de plans de gestion transversaux ou de modalités d'alerte inter-réseaux. Conserver l'outil tel qu'il est aujourd'hui et l'intégrer au sein de ce concept global permettrait également de finaliser les 3 dernières phases de son développement, dont une est relative, également, à la conduite d'un exercice de validation.

Ces pistes de travail sont développées dans l'article en annexe et synthétisées dans le tableau 4.1 ci-dessous :

Mettre en place le SAP après avoir contourné les difficultés rencontrées	Destiner le SAP à d'autres usages
<ul style="list-style-type: none"> ▶ Opérationnaliser <i>Domino</i> comme préalable à la mise en place d'un SAP, ▶ Revoir le niveau de détail nécessaire aux exploitants de réseaux et gérer les problématiques de confidentialité, ▶ S'interroger sur le portage adéquat du système pour bénéficier d'une alerte 24/7, ▶ Travailler ressource par ressource pour développer des procédures de gestion transversales. 	<ul style="list-style-type: none"> ▶ Pour de l'assistance à la planification <i>Coupures planifiées, développement d'aide-mémoire, ...</i> ▶ Pour de l'organisation d'exercices <i>Développement de scénarios, répétition de séquences, ...</i> ▶ Pour de l'aide à la décision en gestion de crise <i>Visualisation de la propagation, identification des acteurs clés, ...</i> ▶ Comme outil de sécurité civile <i>En conservant les visualisations pertinentes, sans les aspects problématiques (alerte, mesures de gestion)</i>

Tableau 4.1 : Synthèse des pistes de travail

Au-delà des paradoxes liés à la difficulté de la mise en place d'un SAP au sein de réseaux interdépendants, paradoxes ayant mis en évidence une inadaptation de l'outil au contexte, il nous a paru également intéressant de considérer les difficultés d'implantation d'un système expert et de son extension, le SAP, sous l'angle plus général d'une résistance au changement. Il s'agit ici d'évoquer une piste supplémentaire susceptible de déterminer si la résistance au changement en tant que telle peut être un facteur critique dans l'impossibilité actuelle d'implanter un SAP dans le contexte des réseaux interdépendants. Cependant, le SAP n'ayant pas été implanté, aucun changement ni technique ni organisationnel n'a eu lieu et cette piste n'a pu être validée.

... à de la résistance au changement.

Lorsque Bareil & Boffo postulent que « Qui dit changement, dit résistance au changement » (Bareil & Boffo, 2003), ils ne font qu'appliquer au comportement humain le principe physico-chimique de Le Chatelier qui précise que « lorsque les modifications extérieures apportées à un système en équilibre provoquent une évolution vers un nouvel état d'équilibre, l'évolution s'oppose aux perturbations qui l'ont engendrée et en modère l'effet. »

Lewin, de son côté, détermine que toute action destinée à produire un changement exercée sur un groupe va se voir opposer une résistance afin de maintenir l'équilibre global au prix d'une augmentation des tensions internes (Lewin, 1948). Et plus la pression sera forte, plus la résistance sera élevée.

Lester Coch et John French sont à l'origine de la notion de résistance au changement. Dans l'article « *Overcoming resistance to change* » (Coch & French, 1948), étudiant la résistance des employés de Harwood Manufacturing à la mise en place de nouvelles méthodes de production, ils mettent en évidence que cette résistance est une combinaison de facteurs à la fois individuels liés aux travailleurs eux-mêmes, mais également collectifs, générés par le groupe (Vas & Vandeveld, 2000). Fort de cette constatation, leurs travaux ont alors porté sur la compréhension de cette résistance mais également les moyens de la surmonter.

Plus récemment, de nombreux travaux sur la résistance au changement organisationnel ont donné lieu à plusieurs définitions. Pour Morin, il s'agit « des forces qui s'opposent à la réorganisation des conduites et à l'acquisition des nouvelles compétences ou, en d'autres mots, à des forces restrictives » (Morin, 1996); pour Dolan et al., il s'agit de « l'attitude individuelle ou collective,

consciente ou inconsciente, qui se manifeste dès lors que l'idée d'une transformation est évoquée. Elle représente donc une attitude négative adoptée par les employés lorsque des modifications sont introduites dans le cycle normal de travail » (Dolan, Lamoureux, & Gosselin, 1996). Ces deux définitions à connotation négative envisagent donc toute résistance au changement comme un refus de changement. De leur côté, certains auteurs voient plusieurs avantages à faire face à une certaine résistance et proposent d'utiliser cette résistance plutôt que d'essayer de la vaincre (Waddell & Sohal, 1998). Ils postulent par exemple que tout changement n'est pas forcément bon par nature, et que seul le temps pourra témoigner de sa pertinence. Ainsi, une résistance au changement pourrait traduire la perception par le groupe d'une faiblesse dans le changement annoncé, et provoquer sa modification ou son retrait. Finalement, la résistance au changement pourrait amener à choisir de nouvelles alternatives (Hayes, 2000). Piderit, de son côté, note qu'une « divergence d'opinions est nécessaire afin que les groupes prennent des décisions éclairées et que les organisations changent efficacement. » (Piderit, 2000) (Traduction libre).

Collerette et al., pour leur part, définissent la résistance comme étant « l'expression implicite ou explicite de réactions de défense à l'endroit de l'intention de changement » (Collerette, Delisle, & Perron, 1997). Cette dernière définition a le mérite de faire le lien entre le changement en tant que tel et la perception du changement par l'individu. Il est envisageable que des mécanismes conscients ou inconscients basés sur le vécu, l'éducation ou la culture confèrent au changement auquel l'individu est confronté des caractéristiques plus ou moins agressives ou déstabilisantes, et ainsi, excluant tout critère objectif, conditionnent un refus destiné en premier lieu à se protéger.

Les freins au changement

De nombreuses causes de résistances au changement ont été identifiées. Bareil, par exemple, les classe en six catégories (Bareil, 2004a) : les causes individuelles, les causes collectives ou culturelles, les causes politiques, celles liées à la qualité de mise en œuvre du changement, à l'organisation dans laquelle le changement survient et enfin, au changement en lui-même.

Deux de ces catégories seront écartées des causes probables de résistance à la mise en place d'un SAP en environnement technologique :

- Les causes collectives et culturelles, regroupant la perte de droits acquis, les normes sociales, les valeurs culturelles ou les valeurs, rites, et histoire,

- Les causes politiques, regroupant les notions de pression politique ou syndicale et de soutien à une cause.

1. Les causes individuelles

La résistance d'un individu au changement traduit une appréhension vis-à-vis de la nouveauté, une crainte de voir changer l'environnement qu'il contrôle, une peur de voir émerger des conflits ou une hostilité face à un changement qu'il lui paraît ne pas être capable de maîtriser (Collerette, et al., 1997). La résistance est alors un mécanisme de défense servant à diminuer l'anxiété que l'individu perçoit dans la transition entre un environnement connu et maîtrisé, et un changement source d'incertitude (Bareil, 2004b).

La notion de « mécanisme de défense » renvoie aux recherches de Hans Selye sur le stress au cours des années 1930 qui se décrit comme « une réaction d'alarme, de mobilisation et de défense de l'individu face à une agression ou une menace » (Crocq & Lery, 1989). Alors que le stress n'est pas uniquement lié aux situations associées aux relations humaines mais survient dans l'ensemble des changements auxquels l'individu est confronté (voyage, décision, maladie, événement familial, etc.), Paulhan & Bourgeois postulent que le contrôle qu'opère l'individu sur son environnement dépend de sa perception de la situation et en particulier de son niveau de responsabilité dans l'événement (hasard, malchance, non préparation, responsabilité personnelle, etc.) (Paulhan & Bourgeois, 1995), générant ainsi un niveau de stress plus ou moins élevé. Sa réponse sera alors fonction de critères individuels émotionnels et donc subjectifs; elle peut être négative si l'individu estime que sa responsabilité personnelle, par exemple, est trop engagée.

Pour Alain, d'autres causes de résistance résident dans la préférence pour la stabilité ou le manque de motivation (Alain, 1996). De manière générale, il apparaît que l'individu en lui-même soit porteur d'une certaine inertie face au changement. Changer demande à la fois un effort et une remise en cause, réticences qui ne seront vaincues que lorsque le changement en question sera perçu comme un réel gain pour celui qui le mettra en œuvre.

2. Les causes liées à la qualité de la mise en œuvre du changement

« Le succès d'une transformation n'est pas qu'une question de disposition positive des acteurs concernés, il faut aussi développer les capacités individuelles et organisationnelles nécessaires à sa réalisation. L'habilitation permet d'équiper les acteurs pour réaliser le changement. » (Rondeau, 2002)

Ainsi, le succès d'un changement ne serait pas lié à ses caractéristiques intrinsèques mais à la façon dont il est implanté. Lorsqu'il s'agit d'un outil technologique tel qu'un SAP, ce ne serait pas les difficultés techniques liées à son implantation ni même son coût qui freineraient sa mise en œuvre, mais la façon dont l'outil est présenté et la façon dont il va s'insérer dans le contexte existant. Les principales résistances pourront alors provenir des facteurs suivants :

- Le changement est imposé, auquel cas les individus vont être immédiatement – et par principe – résistants,
- Le changement n'a pas fait l'objet de consultations, les participants n'y sont pas préparés, et ne se sentent alors pas suffisamment concerné pour trouver un intérêt dans le changement et l'appuyer,
- Le changement n'a pas été suffisamment documenté, et les participants manquent d'informations pour se faire une idée claire de ce qu'il va apporter et comment l'implanter,
- Le changement implique des pratiques nouvelles qui n'ont pas été prises en compte, par exemple la création et la gestion d'un budget spécifique, ou la formation nécessaire à l'emploi de l'outil,
- Les participants n'ont pas l'autorité pour mettre en œuvre le changement.

3. Les causes organisationnelles

La résistance au changement peut également provenir des caractéristiques de l'organisation dans laquelle il s'insère. Lorsque l'on s'intéresse aux organisations, il convient de distinguer 2 concepts (Joule & Beauvois, 2002) :

- Ce qui a trait à la structure de l'organisation et à ses objectifs, dont les individus ont le plus souvent une idée claire et qui induisent de leur part le plus généralement des comportements stables liés à la perception qu'ils ont de la structure,
- Ce qui a trait à la culture de l'organisation, ses mœurs, ses modes de fonctionnement, pour lesquels il y a autant d'avis que d'individus quant à la perception de la hiérarchie, les rapports humains, des motivations. De plus, ces perceptions auront tendance à varier avec le temps.

Dans le premier cas, l'organisation sera jugée comme plutôt inerte ou à l'inverse plutôt flexible, ce qui va conditionner la volonté des individus la composant à vouloir implanter un changement. Plus l'organisation apparaîtra comme inerte, plus le changement apparaîtra comme improbable voire impossible, et moins l'individu s'impliquera dans une telle démarche (Bareil, 2004b).

Dans le deuxième cas, la tendance naturelle de l'individu sera de ne pas se désolidariser de la position admise par le groupe. Cette position est susceptible de fluctuer avec le temps, selon les gens en place et les pratiques admises. Ainsi, une structure avec une hiérarchie ouverte aux innovations, des chefs de service moteurs de changement et des équipes de travail soudées, a davantage de chances de voir s'implanter un nouvel outil, puisque l'apport de nouveauté sera considéré comme une pratique admise, voire souhaitable, par l'ensemble du groupe et donc, par extension, par chacun des membres qui le composent. Le groupe, par nature, demeure solidaire, et c'est solidairement qu'il mettra en œuvre sa capacité de changement (Lewin, 1948).

4. Les causes liées au changement en lui-même

Le changement par lui-même peut être cause de résistance.

En premier lieu parce qu'il pourrait être perçu comme ne servant à rien (Bareil, 2004b). Échec de l'implantation d'un précédent changement de même type, manque d'information sur les avantages attendus, inadéquation apparente entre le changement annoncé et les besoins de la structure, les raisons peuvent en être multiples.

En second lieu parce que les individus ont tendance aujourd'hui à résister non pas au changement, mais *aux* changements. Le changement deviendrait en effet la norme et la continuité, l'exception. Comme le précise Abrahamson, dans le cas où l'organisation met en place de nombreux changements, souvent plus qu'elle ne peut en gérer, les individus, voyant leur charge de travail augmenter sans que les projets initiés parviennent à leur fin, auront une tendance naturelle à refuser tout changement supplémentaire (Abrahamson, 2004). Cette situation est susceptible de générer une certaine anxiété et de nombreux bouleversements, les individus ayant des difficultés, au sein de multiples changements, à dissocier ce qui est important de ce qui ne l'est pas, à déterminer quelle conduite tenir ou quelle procédure suivre, ou encore à savoir vers qui se tourner et dans quel cas.

Finalement, la structure aura de plus en plus de difficulté à mettre en place des changements, fussent-ils importants, chaque nouveau changement ralentissant la mise en place des précédents,

qui parfois même ne seront pas menés jusqu'à leur fin, amplifiant ainsi pour les individus le sentiment d'échec d'une telle politique.

Surmonter la résistance au changement

Pour surmonter la résistance au changement, plusieurs approches sont possibles.

Pour Kotter et Schlesinger, l'implantation réussie du changement passe par de la formation, de la communication, la participation et l'implication, la facilitation et le support, la négociation et la manipulation (Kotter & Schlesinger, 1979). Alain, de son côté, réduit les approches à 4, la communication, la compréhension, la facilitation et la responsabilisation (Alain, 1996). Lewin, développant sa théorie des champs de force, propose soit d'augmenter les forces motrices, soit de diminuer les forces défavorables, soit d'agir sur les deux (Lewin, 1943). Une autre approche intéressante est proposée par Collerette, Delisle et Perron qui suggèrent dans certains cas de retirer le projet et de le représenter dans un contexte plus favorable (Collerette, et al., 1997).

Pour autant, croire que vaincre les freins connus au changement provoque automatiquement la disparition de toute résistance serait une vision réductrice des caractéristiques intrinsèques de l'être humain, par nature changeant, sensible au subjectif et à l'influence de son environnement social, familial, ou professionnel. Sa décision de demain ne sera pas forcément celle d'aujourd'hui, rien ne sera jamais acquis et toute avancée pourra toujours être remise en question. La résistance « constitue souvent le compagnon paradoxal de l'agent de changement, et celui-ci doit s'attendre à devoir fréquenter ce compagnon aussi longtemps qu'il sera porteur de changement » (Collerette, et al., 1997).

Cependant, conscient qu'il n'existe aucune méthode infaillible permettant à coup sûr de vaincre l'ensemble des résistances à l'implantation d'un nouvel outil technologique, il est possible d'envisager plusieurs pistes de travail permettant de faire face à la plupart des facteurs d'opposition décrits précédemment. Ces pistes se traduiraient en pratique par une approche graduelle, destinée d'une part, à vaincre le sentiment d'incertitude lié à cette évolution, et d'autre part, à surmonter les inerties individuelles et collectives.

Dans l'état actuel du projet, il n'apparaît pas que la résistance au changement soit l'un des obstacles majeurs à son implantation, même si cet aspect est aujourd'hui latent et doit être gardé en mémoire pour des travaux futurs. En effet, pour qu'il y ait résistance au changement, il faut

d'abord qu'il y ait changement. L'arrêt du développement du SAP et le fait qu'il n'ait pu être ni implanté, même à titre expérimental, ni testé, n'a apporté aujourd'hui aucun changement à aucun niveau, et n'offre donc pas vraiment un contexte favorable au développement d'une résistance. En revanche, lorsque des travaux sur le SAP seront plus avancés, lorsque les paradoxes évoqués précédemment auront été vaincus et que le contexte de travail permettra l'opérationnalisation de la maquette, il est très probable qu'une résistance au changement verra le jour sous une forme ou une autre. Les diverses études sur la résistance au changement montrent en effet que dans certaines circonstances, le fait de disposer d'un outil même parfaitement adapté au contexte ne garantit pas pour autant le succès de sa mise en place.

CONCLUSION ET RECOMMANDATIONS

La méthodologie d'évaluation des interdépendances développée par le CRP est un outil simple s'appliquant à un environnement au fonctionnement complexe. En effet, même si la création d'un espace de coopération regroupant les exploitants de réseaux a permis de modéliser leurs interdépendances, le développement du SAP a mis en évidence certaines limites à la précision des résultats et une inadéquation entre les résultats obtenus et les résultats attendus. Pour autant, ces travaux auront contribué à isoler les causes de ces difficultés et à identifier un certain nombre de pistes destinées à les contourner.

La revue de littérature a mis en évidence qu'il n'existe aujourd'hui ni définition universelle d'un SAP, ni composition formelle, et que chaque système développé doit prendre en compte l'environnement qui le supporte ainsi que la fonction à laquelle il est destiné. Ainsi, appliqués à la problématique du CRP, ces travaux ont permis de donner une définition particulière de l'outil ainsi qu'une caractérisation de sa composition. Il a été également déterminé que l'efficacité d'autres SAP pouvait être évaluée à l'aide des mêmes critères, ce qui tendrait à démontrer qu'il est possible de définir la composition d'un SAP de manière générale, quelque soit l'environnement dans lequel il doit être implanté.

Les objectifs de recherche prévoyaient le développement complet du SAP, de sa création à sa validation, et postulaient qu'un tel système permettrait d'améliorer de façon significative la qualité et le délai de réponse aux défaillances se propageant au sein de réseaux interdépendants. Même si ces objectifs n'ont pu être vérifiés, les travaux de recherche ont permis des avancées intéressantes dans plusieurs domaines :

- Du point de vue de l'outil en lui-même, il a été possible de développer une maquette à partir des informations enregistrées dans *Domino*. Cette maquette propose plusieurs visualisations utiles à la fois pour les exploitants de réseaux, la Sécurité civile et les services gouvernementaux s'il s'agissait de faire face à une défaillance majeure ayant des conséquences sur une proportion significative de la population et un grand nombre de réseaux ou de services. Elle a également permis de mettre en évidence les différents effets

que peut engendrer la propagation d'une défaillance, contribuant ainsi à une meilleure connaissance du système dans son ensemble.

- D'un point de vue plus conceptuel, il a été possible de détailler les composantes d'un SAP et de déterminer les informations indispensables à son efficacité. Plusieurs SAP pouvant être analysés au vu de ces mêmes composantes, comme cela a été réalisé dans l'article en annexe, une partie des présents travaux pourront être transposés à divers autres systèmes afin d'en améliorer le niveau d'efficacité ou d'en déterminer les causes d'une potentielle inefficacité.

Le développement du SAP a également permis de souligner la nécessité de la mise en place de mesures de gestion transversales inter-réseaux. Alors que les procédures de gestion des défaillances sont aujourd'hui internes à chacun des réseaux, la mise en évidence des modalités de propagation d'une défaillance ainsi que le nécessaire emploi d'une quantité limitée de RA amènent à repenser la gestion des défaillances aux bornes du système considéré. Cet élargissement de la vision d'un niveau d'ensemble fonctionnel à un niveau systémique met en évidence que l'interconnexion des différents ensembles nécessite la mise en place de procédures de gestion également interconnectées.

D'une manière plus globale, ces travaux ont permis de repenser, ou à tout le moins d'entamer une réflexion sur le contexte de collaboration entre le CRP et les réseaux partenaires en vue de l'approche à adopter dans les travaux futurs. Après avoir mis en évidence que la qualité des résultats attendus était en inéquation avec la qualité des informations fournies, il a été possible de proposer plusieurs pistes visant à améliorer la collaboration entre les exploitants de réseaux et le CRP, tout en préservant une nécessaire confidentialité des données. Cette collaboration renforcée devrait bénéficier à l'ensemble de l'espace de coopération en ce qui concerne la gestion des défaillances de leurs réseaux.

Enfin, sachant qu'une telle démarche d'amélioration prendra du temps, il a été possible de définir pour le court terme d'autres utilisations du SAP afin de capitaliser sur les résultats déjà obtenus.

Les utilisations proposées dans l'article en annexe s'insèrent dans ce que Gralepois définit comme de la « vigilance de territoire » (Gralepois, 2010). Partant du postulat qu'une interruption de service de réseaux urbains (voirie, canalisations, câblage, etc.) même si elle se présente comme une panne gérable localement, peut néanmoins s'aggraver jusqu'à devenir une véritable

situation de crise, elle doit être, à ce titre, encadré par des outils de sécurité civile. Le SAP qui, grâce aux visualisations qu'il propose, permet d'anticiper sur les conséquences dans l'espace et dans le temps d'une défaillance initiale, se range dans cette catégorie d'outils. Cette constatation peut amener un point de vue intéressant lorsqu'il s'agira de définir le futur portage du système expert *Domino*.

LISTE DE RÉFÉRENCES

- Abrahamson, E. (2004). Avoiding Repetitive Change Syndrome. *Harvard Business Review*(December).
- Agence France Presse [AFP]. (2011). *Pétrole: facture mondiale record en 2011*. Consulté le 20 mai 2011, tiré de <http://www.jdf.com/flash-bourse/2011/03/04/97002-20110304FILWWW00483-petrole-facture-mondiale-record-en-2011.php>.
- Alain, M. (1996). *Prendre en main le changement – Stratégies personnelles et organisationnelles*. Montréal: Éditions Nouvelles.
- Bareil, C. (2004a). *Gérer le volet humain du changement*. Montréal: Éditions Transcontinental.
- Bareil, C. (2004b). *La résistance au changement : synthèse et critique des écrits*. Montréal: HEC.
- Bareil, C., & Boffo, C. (2003). Qui dit changement, dit préoccupation et non plus résistance. In G. Karnas, C. Vandenberghe & N. Delobbe, (Éds.), *Bien-être au travail et transformation des organisations: Actes du 12e congrès de psychologie du travail et des organisations* (Vol. 3, pp. 541-551). Louvain: Presses universitaires de Louvain.
- BBC News. (2006). Asia tsunami warning system ready. Retrieved from <http://news.bbc.co.uk/2/hi/asia-pacific/5126710.stm>
- Bussière, M., & Fratzscher, M. (2002). *Working paper #145 : Towards an early warning system of financial crisis*. Working Paper Series. European Central Bank. Retrieved from www.ecb.int
- Centre d'Expertise Hydrique du Québec [CEHQ]. (2011). *Champs d'activité du CEHQ*. Consulté le 21 juin 2011, tiré de http://www.cehq.gouv.qc.ca/champs_acti/index.htm.
- Centre de Prévision des Crues du Québec [CPCQ]. (2011). *Prévisions d'un évènement météorologique perturbateur*. Consulté le 21 juin 2011, tiré de http://www.hydrometeo.com/index.php?option=com_content&task=view&id=31&Itemid=9.
- Coch, L., & French, J. R. P. J. (1948). Overcoming Resistance to Change. *Human Relations*(1), 512-532.
- Collerette, P., Delisle, G., & Perron, R. (1997). *Le changement organisationnel : théorie et pratique*. Sainte-Foy: Presses de l'Université du Québec.
- Commission des Communautés Européennes. (2005). *Livre vert sur un programme européen de protection des infrastructures critiques*. COM(2005) 576 final. Consulté le 12 décembre 2010, tiré de http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=COMfinal&an_doc=2005&nu_doc=576

- Crocq, L., & Lery, O. (1989). *Le stress des décideurs et des sauveteurs dans les catastrophes*. Paper presented at the Congrès de psychiatrie et neurologie de langue française. LXXXVIIème session. , Montreal.
- Department of Homeland Security [DHS]. (2009). *National Infrastructure Protection Plan*. Consulté le 11 mai 2011, tiré de http://www.dhs.gov/files/programs/editorial_0827.shtm.
- Dolan, S. L., Lamoureux, G., & Gosselin, E. (1996). *Psychologie du travail et des organisations*. Montréal: Gaëtan Morin.
- Emergency Events Database [EM-DAT]. (2009). *Natural Disasters Trends*. Consulté le 11 mai 2011, tiré de <http://www.emdat.be/natural-disasters-trends>.
- Federal Emergency Management Agency [FEMA]. (2004). *Federal Guidelines for Dam Safety*. Washington, D.C.: Interagency Committee on Dam Safety.
- Federation of American Scientists. (2011). *Ballistic Missile Early Warning System*. Consulté le 15 janvier 2011, tiré de <http://www.fas.org/spp/military/program/track/bmews.htm>.
- Gralepois, M. (2010). L'agglomération à flux tendus. La politique de sécurité civile française au secours des pannes urbaines. *Flux*, 81(Juillet-Septembre 2010), 57-66.
- Hayes, T. A. (2000). *Constructive Derivatives From Resistance to Change in Organizations: A Literary Review*. Point Loma Nazarene University. Retrieved from www.timhayesweb.com
- Joule, R. V., & Beauvois, J. L. (2002). *Petit traité de manipulation à l'usage des honnêtes gens*. Grenoble: PUG.
- Kjellén, S. K. (2009). Crisis Management in the European Union. In S. Olsson, (éd.), *Rapid Alerts for Crises at the EU Level*. Berlin-Heilderberg: Springer-Verlag.
- Kotter, J. P., & Schlesinger, L. A. (1979). Choosing strategies for change. *Harvard Business Review*(mars-avril), 106-114.
- Lewin, K. (1943). Defining the field at a given time. *Psychological Review*, 50, 292-310.
- Lewin, K. (1948). *Resolving social conflicts*. New York: Harper and Row Publishers.
- Mallet, J. C. (2008). *Livre Blanc de la Défense et de la Sécurité Nationale*. Paris: La Documentation Française. Retrieved from www.livreblancdefenseetsecurite.gouv.fr/.
- Ministère de l'Intérieur. (2011). *L'alerte et l'information des populations*. Consulté le 24 janvier 2011, tiré de www.interieur.gouv.fr.
- Ministère de l'Intérieur et de l'Aménagement du Territoire. (2007). *Arrêté du 23 mars 2007 relatif aux caractéristiques techniques du signal national d'alerte*. Paris, France.

- Ministère de la Santé et des Services Sociaux [MSSS]. (2011). *Plan chaleur accablante*. Consulté le 10 février 2011, tiré de www.msss.gouv.qc.c.
- Morin, E. M. (1996). *Psychologies au travail*. Montréal: Gaëtan Morin.
- Office of Rail Regulation. (2011). *The Automatic Warning System*. Consulté le 16 janvier 2011, tiré de <http://www.rail-reg.gov.uk/server/show/nav.1558>.
- Organisation du Traité de l'Atlantique Nord [OTAN]. (2007). *AWACS : les yeux de l'OTAN dans le ciel*. Consulté le 16 janvier 2011, tiré de <http://www.nato.int/issues/awacs/practice-f.html>.
- Ozer, P., & De Longueville, F. (2005). Tsunami en Asie du Sud-Est : retour sur la gestion d'un cataclysme naturel apocalyptique. *Revue européenne de géographie*, 321(14 octobre 2005).
- Paulhan, I., & Bourgeois, M. (1995). *Stress et coping : les stratégies d'ajustement et l'adversité*. Paris: PUF.
- Piderit, S. K. (2000). Rethinking resistance and recognizing ambivalence: A multidimensional view of attitudes toward an organizational change. *The Academy of Management Review*, 25, 783-795.
- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(2001), 11-25.
- Robert, B. (2009). *Résilience organisationnelle : concepts et méthodologie d'évaluation*. Montréal: Presses internationales polytechnique.
- Robert, B., De Calan, R., & Morabito, L. (2008). Modelling Interdependencies Among Critical Infrastructures. *International Journal of Critical Infrastructures*, 4(4), 392-408.
- Robert, B., & Morabito, L. (2009a). Dependency on electricity and telecommunications. In M. Weijnen, Z. Lukszo & G. Deconinck, (Éds.), *Securing electricity supply in the cyber age: Exploring the risks of information and communication technology in tomorrow's electricity infrastructure*. (pp. 34-55): Springer.
- Robert, B., & Morabito, L. (2009b). *Réduire la vulnérabilité des infrastructures essentielles : guide méthodologique*. Paris: Tec&Doc.
- Robert, B., & Morabito, L. (2010). An approach to identifying geographic interdependencies among critical infrastructures *Int. J. Critical Infrastructures*, 6(1), 17–30.
- Robert, B., Morabito, L., & Quenneville, O. (2007). The preventive approach to risks related to interdependent infrastructures. *International Journal of Emergency Management*, 4(2), 166-182.

- Rondeau, A. (2002). Transformer l'organisation. Vers un modèle de mise en œuvre. In R. Jacob, A. Rondeau & D. Luc, (Éds.), *Transformer l'organisation* (pp. 91-112). Montréal: HEC.
- Secrétariat Général de la Défense et de la Sécurité Nationale [SGDSN]. (2011). *Vigilance, prévention, protection : le plan Vigipirate*. Consulté le 8 janvier 2011, tiré de www.sgdsn.gouv.fr.
- Sécurité Publique Canada. (2010). *Infrastructures essentielles*. Consulté le 14 janvier 2011, tiré de <http://www.securitepublique.gc.ca/prg/em/ci/index-fra.aspx>.
- Time Magazine. (1963). *Defense: Sign-off for CONELRAD* Jul. 12, 1963. Consulté le 14 janvier 2011, tiré de <http://www.time.com/time/magazine/article/0,9171,940303,00.html>.
- UN/ISDR. (2006). *Développement de systèmes d'alerte précoce : une liste de contrôle*. Paper presented at the EWC III, Bonn.
- United Nations/International Strategy for Disaster Reduction [UN/ISDR]. (2005). *Cadre d'action de Hyogo 2005-2015 : pour des nations et des collectivités résilientes face aux catastrophes*. Consulté le 8 février 2011, tiré de <http://www.unisdr.org/eng/hfa/hfa.htm>.
- USAID. (2011). *The Famine Early Warning System Network*. Consulté le 17 janvier 2011, tiré de <http://www.fews.net/Pages/default.aspx>.
- Vas, A., & Vandavelde, B. (2000). *La résistance au changement revisitée du top management à la base : une étude exploratoire*. Paper presented at the IXème conférence internationale de management stratégique, Montpellier.
- Waddell, D., & Sohal, A. S. (1998). Resistance: a constructive tool for change management *Management Decision*, 36, 543.

ANNEXE 1 – Article

Cet article, synthèse des travaux de recherche décrits dans ce document, a été soumis pour publication au *Journal of Homeland Security and Emergency Management* (JHSEM).

Publié depuis 2003 par *The Berkeley Electronic Press*, le JHSEM se définit comme une source de première importance de ressources de recherche et d'information sur les sujets de la sécurité intérieure et de la gestion des situations d'urgence. Ces ressources couvrent les domaines des mesures d'urgence, de l'ingénierie, des sciences politiques, des politiques publiques, de la science des processus décisionnels, de la santé et de la médecine. Son rédacteur en chef est Irmak Renda-Tanali, de la *Graduate School of Management & Technology* de l'Université du Maryland (États-Unis). Certains de ses contributeurs proviennent de centres de recherche majeurs tels que *The Centers for Disease Control and Prevention*, *Harvard University*, *Carnegie Mellon University*, *the Environmental Protection Agency*, *George Mason University*, *George Washington University*, *RAND*, et *Vanderbilt University*.

Failures within Interdependent Systems: Challenges Related to Implementing an Early Warning System.

Cédric Debernard, Benoît Robert

Abstract

Operators of critical infrastructures today face a problem: managing failures within systems that are constantly becoming more complex because of the number of related and interdependent infrastructures. Anticipating the consequences of potential failures is a necessity for system operators, in order to limit their impact both on the general public and on the infrastructures themselves. This article presents a project for an early warning system designed to provide information about the propagation of a potential failure in space and time. It emphasizes the difficulty of putting such a system in place in a context of interdependent systems and proposes an alternative that takes the different system operators' expectations, constraints and operating methods into consideration.

1. Introduction

The modernization of our societies, which generates numerous dependencies on multiple resources; the increased complexity of our social, economic and industrial networks; the growth in population density in cities; and the consequences of climate change are just some of the factors characterizing the increase in our modern societies' vulnerability to natural or anthropic hazards. When a weather event, industrial accident or terrorist act occurs, this increased vulnerability is reflected in an increase in the consequences, proportional to the human and technological complexity of the infrastructure in question. And these consequences have numerous characteristics related to scope, effects and persistence. So-called critical infrastructures are vital to the health, safety and well-being of populations, as well as the normal functioning of institutions and the country's economy (Department of Homeland Security [DHS], 2009). They are organized in interconnected and interdependent systems. Thus, a failure that appears in one area of a given system is likely to propagate not only within the same system but also through the other systems with which it is interconnected (Robert & Morabito, 2009). Maintaining their systems' mission by supplying an optimal level of services and resources is a major and constant concern for system operators. For this reason, the *Centre risque et performance* (CRP) developed an expert system for modeling failures within a certain number of critical infrastructures in Quebec (Robert, De Calan, & Morabito, 2008).

This article examines the problem of the propagation of failures within interdependent critical infrastructures and presents a model of an early warning system. This anticipation and warning system would make it possible to inform infrastructure operators of the propagation of a failure, in time and space, thereby enabling them to put a certain number of management measures in place beforehand in order to limit the possible consequences for their own infrastructures and the services they provide for the population.

This article also presents the difficulties of setting up such a system in the context of interdependent systems in Montreal. It identifies the various obstacles to its implementation and notes two major paradoxes involving the definition of an early warning system and the system operators' expectations. In light of the information that the system is able to provide, it suggests a redefinition of its objectives and a new framework for its use.

2. Early warning systems

2.1 Description and definition of an early warning system

Although they have been widely popularized by the media in numerous forms covering a wide range of fields, early warning systems (EWS) appear to be a relatively recent discovery, essentially related to the development of technologies. Nevertheless, in a sense, the concept of an early warning dates back to the dawn of time—even to the origins of life itself. Nature has equipped living beings with a variety of tools to warn them of dangerous situations so that they can take steps to protect themselves. Pain, fear and aposematism (danger signals such as warning coloration) are some examples of such tools.

Events in recent years (Brazil and Japan in 2011, Haiti and Pakistan in 2010, Australia and Italy in 2009, Myanmar in 2008, etc.) remind us that natural disasters always claim their share of victims. With the disastrous aftermath of the Indian Ocean tsunami of December 26, 2004, in mind, two years later the United Nations published the report "Global Survey on Early

Warning Systems,” which showed that thanks to such systems – associated with other planning and response processes – deaths due to natural disasters had declined significantly in the last 30 years (United Nations, 2006).

Although their forms vary, all early warning systems are characterized by a common underlying definition: an EWS is a tool that provides timely and relevant information on the occurrence of a failure, which will make it possible to take steps to limit the consequences.

2.2 Components of an early warning system

To meet this definition, the development of an EWS should, from the outset, take the following aspects into consideration:

- The tool

The tool itself may take many forms. From the smoke signals used by Aboriginal peoples through the road sign to the electronic interface of the Tsunami Warning System, with its interconnected sensors, buoys, antennas and satellites, many possible supports can be contemplated, provided that they provide clear, easy-to-use information on the occurrence and development of a dangerous situation.

- The knowledge of the system and identification of dangerous situations

A health crisis and a flooding river bear little resemblance to each other and produce very different effects. Thus, an EWS can only be designed if it is adapted to a defined context. It is necessary to delimit the environment in which the tool will be set up and to study this environment in terms of its structure, its functioning, its interfaces and the specific dangerous situations that are likely to occur there in order to create an EWS that will meet users' needs.

- The choice of indicators and information presented

The key issue in making such systems effective is to find relevant indicators for which a certain amplitude of variation will trigger a warning. The more sophisticated and fluctuating the system is, the more complicated the search for reliable indicators will be, and the more caution must be applied in interpreting them. This is particularly true of systems that rely greatly on the human factor, which by nature is potentially unpredictable: for example, the activity of terrorist networks. Conversely, the better known and more stable the system is, the more fine-grained the notion of indicator can be and the more relevant its variations are: for example, observation of the change in water levels in a river during an episode of torrential rain constitutes an EWS insofar as, combined with management plans, it will make it possible to implement measures to protect riverside inhabitants, depending on the water level. In all cases, effective information must be:

- timely, that is, it must be delivered at a given time in order to inform stakeholders of how much time or room to maneuver they have available.
- relevant, that is, targeted. If there are too many indicators, the tool becomes unreadable (like a dashboard with too many dials) or inaccurate (the relevant information will be drowned in a sea of useless information). Conversely, if too few indicators are available, the tool will not effectively perform its function.

- **The identification of time periods**

Effective management measures cannot be put in place without considering the time limits for the disruption. Once indicators have been identified, they must be read on a time scale in order to give operators the ability to anticipate the consequences of a dangerous situation, which will be reflected in the implementation of measures to protect people and infrastructures and ensure service continuity. In the example above, the time available before the flood reaches a predetermined critical level will give stakeholders indispensable information for preparing and organizing a possible evacuation.

- **The warning**

One of the main goals of an EWS is to transmit a warning; each warning level must generate an action and mobilize the corresponding resources. When the system is designed, it is therefore necessary to define:

- The conditions for triggering the warning: within the system in question, the structure, hierarchical level and individual responsible for triggering the warning need to be identified, on the basis of evaluation factors – particularly the identification of thresholds – supplied by the EWS.
- The characteristics of the warning that will be transmitted: a single warning or a warning with several levels or with different types for different recipients.
- The mode of transmission: depending on the system studied, several kinds of supports can be envisaged, from very simple to highly complex. The mode may be new or it may be an existing structure into which an early warning function can be integrated.
- The recipients, who are of two types:
 - the stakeholders concerned: these may be the operators of private- or public-sector critical infrastructures, emergency or civil security services, or representatives of administrative or government agencies. Their nature and number will depend on the kind of environment being assessed and on the related political or organizational considerations;
 - the general public: based on the information provided by the EWS, the warning must target the public who will be affected, geographically and over time, to give them information and tell them what to do.

- **The management measures**

An EWS has no value unless the information that it supplies makes it possible to take steps to limit the consequences of a dangerous situation. Thus, the implementation of such a tool must be accompanied by the simultaneous implementation of management plans adapted for the particular dangerous situation. These management plans must cover aspects related to intervention (to limit the consequences of the dangerous situation) and information (for the private- and public-sector stakeholders concerned and for the public).

3. Mastering all the components: A challenge for early warning systems

3.1 Study of two systems

Every EWS is based on the six fundamental components described above. While a number of recently developed EWS did not effectively fulfill their missions (Flynn, 2010; US DHS, 2011b; Vincent, 2010; Voller & Villesen, 2009), a study of the components of these systems makes it possible to identify their weaknesses and understand why they needed to be improved or replaced. This study allows us to learn a number of lessons regarding the obstacles that affect an EWS in a context of interdependent systems.

The two systems we studied were the U.S. HSAS (Homeland Security Advisory System) and the WHO's (World Health Organization) warning system for pandemic flu.

3.2 Summary table of components

	HSAS	WHO
Tool	Indicator of warning levels (1 to 5) in the form of colors.	Indicator in the form of a 6-point scale.
Knowledge of the system and identification of dangerous situations	Variable, depending on specialized agencies' analysis capacities.	Debatable, depending on epidemiological criteria established by the SAGE experts.
Choice of indicators and information presented	Confidential indicators. No geographic limits to the threat. Systematically high warning level (3 or 4 out of 5) Difficulty scaling down warning levels.	Mismatch between warning levels and reality on the ground.
Identification of time periods	No.	No.
Transmission of warning	Yes, by the media (general public) or direct liaison (federal agencies)	Yes, by the national health authorities via the media and the health care systems.
Associated management measures	No indication for the public of what to do.	Excessive measures in relation to the reality of the spread of the virus. Lack of transparency regarding decision-making.

Table 1: Comparison of the components of the HSAS and the WHO's EWS

The analysis of table 1 highlights the fact that the absence or inaccuracy of certain components has a direct impact on the effectiveness of an EWS:

- **The knowledge of dangerous situations is biased**

In the area of security-related information, the available information is directly related to the ability of the various departments involved to collect information and collate it in a summary that will be transmitted to decision-makers so they can make informed decisions (CIA, 2010). Such

information is often inaccurate, piecemeal or unconfirmed, which limits the relevance of the ensuing summary. Decision-makers are therefore forced to act in a context of considerable uncertainty, which has a direct effect on the soundness and quality of the measures imposed.

In the case of the WHO, the low number of victims compared to the seasonal flu led some observers to posit collusion between the pharmaceutical laboratories providing the vaccine and the WHO, which had escalated its warning levels in the absence of any objective epidemiological criteria in order to pressure governments to set up vaccination campaigns (Vincent, 2010). An investigation by two Danish journalists revealed that several members of the Strategic Advisory Group of Experts (SAGE) who were supposed to advise the WHO on the management of pandemic flu were also being compensated by the pharmaceutical laboratories manufacturing the vaccines (Voller & Villesen, 2009). If certain advisors acted without objective epidemiological criteria, then the indicator is automatically invalidated.

- The indicators chosen and the information presented are not relevant

In the case of the HSAS, the level of risk indicated was usually significant, generally 3 or 4 (Elevated or High) on a scale of 5, and the geographic limits of the risk were not identified. This obliged governments and infrastructure operators to adopt a constantly high protection level for the whole territory and gave the impression that insecurity had become the norm. As a result, it tended to desensitize the 300 million U.S. citizens to potential announcements of increased risk. In parallel, although it is relatively obvious that awareness of a threat will generate an increase in the warning level and the application of the related measures, it is difficult for managers to decide to lower the warning level – and thus to reduce protective measures – insofar as, in the security field, the absence of new data does not necessarily correspond to a reduction in the threat.

As for the WHO, and for the same reasons mentioned above, the warning level indicator had no relationship with the reality on the ground.

- No time period is indicated

Neither system included any concept of time in the warning. Instead, the warning was triggered for an indeterminate period, until the available information made it possible to cancel it. In such a context, it is difficult to put adapted management measures in place.

- The systems do not apply relevant management measures

The HSAS was intended essentially for official organizations: its mission was to inform federal departments and agencies of the protective measures to put in place as a function of the corresponding warning level (US DHS, 2002). With regard to the general public, the system was reduced to awareness of a level of risk, without any indication of how to act.

In the case of the WHO, neither the warning levels nor the management measures applied corresponded to the actual consequences. British Member of Parliament Paul Flynn, author of a report to the Council of Europe on the management of the pandemic, said he was “particularly alarmed by some of the excessive responses given to what turned out to be an influenza of moderate severity, and also the lack of transparency of relevant decision-making processes” (Flynn, 2010).

3.3 Fate of the two systems

In the case of the HSAS, the lack of relevant information transmitted to government agencies and the general public was highlighted in 2009 by a committee of experts who were brought together at the request of the Secretary of Homeland Security, Janet Napolitano (US DHS, 2011b). Their conclusions led to the abolition of the HSAS set up in 2002, and its replacement in 2011 by the National Terrorism Advisory System (NTAS). This system, which has only two levels (Imminent threat or Elevated threat), allows for a warning that is targeted in its contents, in space and in time, and can be used to warn the public, government agencies, emergency services, transportation systems and the private sector (US DHS, 2011a).

For the WHO, the numerous reports testifying to the mismatch between warning levels and the management measures associated with the actual spread of the virus led the organization to review its preparations and actions in case of a flu pandemic (WHO, 2009).

More generally, our study of the two systems has emphasized the fact that the effectiveness, and therefore the viability, of an EWS depends on a preliminary analysis of the environment in which it will be used, as well as an in-depth reflection process on the elements that must go into building the different components. In particular, it is necessary:

- to have indicators for each component, without exception;
- for these indicators to be timely and reliable so that the system will be able to produce precise thresholds that will generate rigorous warnings, enabling appropriate – in terms of space and time – management measures to be implemented.

4. The problem of interdependent systems

4.1 Critical infrastructures and interdependencies

To function properly, every industrialized country needs to make daily use of a certain number of human, material and intangible resources supplied by different entities, which themselves can only function thanks to other resources supplied by other entities (Robert & Morabito, 2009).

Among these entities, critical infrastructures (CIs) are characterized as “processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government.” In Canada, these CIs are grouped into 10 categories (Public Safety Canada, 2010): Energy and utilities, Information and communications technology, Finance, Health care, Food, Water, Transportation, Safety, Government, and Manufacturing.

Numerous recent events, and the consequences they triggered, have highlighted the importance of studying the interdependencies among critical infrastructures and the means of limiting the consequences of a potential failure as much as possible. The blackout that affected northeastern North America in August 2003, with its repercussions on almost all critical sectors, is a clear example (Public Safety and Emergency Preparedness Canada, 2006).

4.2 Study of interdependencies by the CRP

For many years, the CRP of the École polytechnique de Montréal has been developing an approach to studying interdependencies.

The most recent research project began in 2008 in both Montreal and Quebec and is continuing until 2012. It has enabled the development of an expert system for modeling the propagation, in time and space, of a failure within a set of interdependent systems. This expert system, known as *Domino*, was produced in partnership with the main CIs – electricity, natural gas, telecommunications, transportation, drinking water – and with the civil security department. It is now able to identify the consequences of an initial failure for different interdependent systems, with a particular emphasis on potential domino effects. Its imaging is based on the geographic grid usually used by the CRP (Robert & Morabito, 2009).

The infrastructure managers agreed that the better they know the systems, their vulnerabilities and the consequences of a failure, and the more advance notice they have before a failure appears, the better able they are to implement effective management and mitigation measures. From this perspective, the CRP's partners considered it to be important to integrate the development of an EWS into its work.

5. An early warning system applied to interdependent systems

5.1 Development of a model

A model of the EWS was developed during the first six months of 2010 (Debernard, 2011). The imaging that it presents is based on the information provided by the partner systems and recorded in the *Domino* expert system, namely the systems concerned, the geographic sectors and the time periods. The model consists in combining the various information available in order to obtain different images that will be presented to the partners and then retained or set aside, depending on their interests.

Thus, the model is able to propose different kinds of imaging as a function of the client. For example, a system operator might wish to focus on its system's interconnections with other interdependent systems in order to warn the latter in case of a failure, whereas Civil Security might want precise information on the geographic propagation of degradations so it can meet the population's needs as well as possible.

The model developed combines several kinds of imaging that are fundamental to implementing appropriate management measures:

- An image of the *systems concerned*, so that their operators can implement specific or cross-cutting management plans to handle failures;
- An image of the *geographic sectors concerned* – images based on the grid of the Island of Montreal – to obtain a fine-grained assessment of the consequences for infrastructures and populations and be better able to manage the use of alternative measures or resources;
- An image of the *time periods* in order to allow operators to better anticipate the scope and sequencing of the actions to be taken to handle failures.

As well, the combination of different images revealed five kinds of effects of a failure on the systems:

Effects on interdependent system: the initial interruption of a resource has a direct effect on the other systems with which the initial system is functionally interdependent.

Effects on dependent systems: the initial interruption of a resource has an effect on the other systems that need that resource to function but are not functionally interdependent with the initial system.

Domino effects: the initial interruption of a resource has an effect on a second system that is interdependent with a third system. The degradation in the third system's service is only indirectly linked to the initial outage.

Rebound effects: the cascade of successive effects finally has a new impact on the system where the initial interruption originated.

Cumulative effects: Without effective management, the degradation will continue to propagate within the dependent and interdependent systems following the 4 previous effects. All systems are liable to affect and be affected by the others in a snowball effect that is difficult to predict given the number of systems affected and the complexity of their interconnections.

5.2 Proposal for implementation in Montreal

The project to implement an EWS for the interdependent systems in Montreal faced numerous difficulties. In the end, the conclusions of a final meeting concerning the guidelines to give the project made it clear that putting an EWS in place no longer represented a priority for the system operators.

These conclusions led the CRP to question the relevance of the model it had developed and consider it through the prism of the system's coherence with the six essential components of any EWS:

Tool	Based on the <i>Domino</i> expert system. Imaging with Excel©, with a transfer to Google Earth© under study
Knowledge of the system and identification of dangerous situations	Within the limits of the information provided by the system operators. The failure of a resource is identified but without precise information about its location.
Choice of indicators and information presented	Indicators' relevance limited by the precision of the data provided by the system operators. No identification of thresholds triggering warnings. Relatively inaccurate geographic imaging due to use of flexible cartography.
Identification of time periods	Yes, integrated into imaging.
Transmission of warning	No identification of which structure and which hierarchical level is in charge of triggering the warning. Difficulties with identification of recipients and modes of transmitting the warning in light of each system operator's internal procedures.
Associated management measures	Makes a certain amount of information available but does not suggest what actions to take. Need for cross-cutting management measures among interdependent systems and difficulties identifying measures to put in place for each system.

Table 2: Study of EWS components for interdependent systems

As in the study of the two earlier systems, table 2 shows that the lack or imprecision of certain components has a direct impact on the EWS's effectiveness:

- Knowledge of the system and of dangerous situations is inadequate because the data precision needed for the imaging is limited by the system operators;
- The choice of indicators is not optimal, in particular because they do not identify any warning threshold that should trigger the implementation of adapted management measures;
- The systems' operating mode makes it impossible to identify which structure and which hierarchical level is responsible for triggering warnings;
- The information provided does not allow users to formally identify the management measures to be put in place by the individual systems, and still less across all the various systems concerned.

6. Analysis and avenues for future work

6.1 Paradoxes in the implementation

Along with the creation of an expert system, the development of an EWS represented one of the main objectives of the 2008–2012 project. However, the presentation of the model to the partners

and the subsequent discussions concerning the execution of the project highlighted the fact that the context of the interdependent systems is not well adapted to the implementation of an EWS. Two major paradoxes were identified:

➤ **First paradox**

Although the implementation of an EWS arose out of a need expressed by the partner systems and was the subject of an explicit request on their part, today none of the partners seems to wish to launch such an initiative.

The data used by the EWS comes from the *Domino* expert system created by the CRP. The technical and geographic information provided by the various systems feeds into it. The partners now question the long-term viability of the tool, which is now supported by the CRP but will eventually require a decision regarding the organization that will have to manage its use, as well as the staff, budget and management plan needed for its continued operation, bearing in mind the fact, with an eye to future development, that the greater the number of partner systems or the higher the level of detail required on each infrastructure, the more data will have to be stored and processed. Since the EWS is viewed as an extension of *Domino*, it appears crucial to first ensure the operationalization of the expert system before considering the further development of an EWS.

The EWS is seen as a new tool that will be difficult to implement. The tool in and of itself appears to be complex and its value is unclear. Indeed, each system considers itself to be ready to respond to failures because it already has its own procedures for managing breakdowns; clearly, the implementation of the EWS will generate cross-cutting management problems that will require the implementation of intersystem management plans and an integrated warning system. The application of such plans seems vague: How will they be superimposed on each system's current procedures? What administrative or IT constraints will accompany the implementation of the tool? What resources are available to put common management measures in place across the systems?

➤ **Second paradox**

The operators of the partner systems expect that the EWS will provide detailed geographic information even though, for reasons of confidentiality, the system is working on the basis of flexible cartography.

Information sharing among the interdependent systems is a necessary condition for modeling their interdependencies and providing data for an EWS. However, for reasons of confidentiality, the systems are reluctant to share precise data, especially geographic data. It was therefore agreed that a grid of the whole Island of Montreal, with 1-km² sectors, would be developed so that the systems could localize their infrastructures without revealing their specific position. *Domino* and the EWS are therefore based on flexible cartography (Robert & Morabito, 2009). This lack of detail, which is a consequence of the partners' initial choice to allow their technical information to be used only in relatively imprecise graphics, raises doubts about the relevance of the EWS images.

This paradox confirms that confidentiality is often an obstacle to inter-organizational work (Cho, 2005; Cutter, 2003; Harvey & Tulloch, 2006).

6.2 A necessary redefinition of the tool

Given the two paradoxes discussed above, the CRP recognizes that it is now necessary to rethink the early warning system as a concept, and not only as a tool. And in order to lay the foundations for this concept, it is necessary to consider the expectations of the interdependent system operators.

- *The EWS as developed in the model does not meet an internal operating need.*

Each system now has its own internal tools and procedures for managing breakdowns. Because it relies on flexible cartography, the EWS does not provide relevant information that would enable the systems to improve their management of their unplanned outages. On the contrary, the system identifies factors that are useful for decision-making in a crisis, namely the system and the sector affected, and especially the consequences for the other interdependent systems and when they will appear. As envisaged today, the EWS would not be used every day by the systems, and its operationalization should be conditioned by openness to other uses than just crisis management, which by its nature is relatively rare.

- *The EWS as developed in the model does not lead to standardized behaviors.*

The system operators expect that the EWS will give them standardized behaviors to apply in different kinds of outages. For this to happen, two conditions are necessary.

The first is that one must be able to define standard behaviors for different kinds of breakdowns that can be translated into applicable operating procedures. However, the silo functioning of the different systems, based on their own internal procedures, and the variability of consequences for all the systems, based on management decisions that are made independently by each one, make it impossible to model with sufficient accuracy the propagation of a failure in time and space and thus come up with a systematically standardized reaction.

The second condition is that it would be necessary to develop cross-cutting procedures for several systems. To do this, an in-depth knowledge of each system's procedures would be needed. For the reasons of confidentiality mentioned above, this approach is not feasible today.

7. Conclusion and recommendations

As we have seen, there is a significant gap between the definition of an EWS – the level of detail of the information needed to develop one – and the system operators' expectations regarding its capacities. Thus, it is necessary to redesign the system not as an EWS – that is to say, a tool that provides timely and relevant information about the occurrence of a dangerous situation, which will make it possible to take steps to limit its consequences – but as the early provision of a set of information for the system operators that will enable them to take more or less formalized action, based both on the knowledge of the failure's propagation and on the internal procedures that govern their interventions. Consequently, the system will no longer be a warning tool but a management tool, with the following missions:

- Assistance with planning

The system should provide information that is directly usable in managing planned outages and developing checklists that present key points in each system's management procedures; these will be integrated into a less detailed inter-organizational document to be used in managing failures across systems.

- Support of drills

By providing information on the propagation of a failure in time and space, the system should provide effective support for the implementation of drill scenarios to train the operators of the interdependent systems to better manage the consequences of failures.

- Assistance with crisis management decisions

When triggered by an actual failure, the system should give system operators and civil security images of the systems affected and the geographic and temporal spread of the failure. These images would make it possible to accurately identify the stakeholders who should be invited to join in the management of the event, the geographic sectors likely to experience the consequences of the failure, and the time available for stakeholders to implement appropriate management measures.

In all cases, the quality of the information provided by this system will depend directly on the level of knowledge that the expert system is authorized to have of the technical and organizational characteristics of each partner system; its precision will be a direct function of the level of detail of the information provided by the system operators.

References

- Cho, G. (2005). *Geographic Information Science: Mastering the Legal Issues*. New York: John Wiley and Sons.
- CIA. (2010). *The Intelligence Cycle*. Consulted on April 14, 2011, retrieved from <https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html>.
- Cutter, S. L. (2003). GI science, disasters, and emergency management. *Transactions in GIS*, 7(4), 439–445.
- Debernard, C. (2011). Défaillances au sein de réseaux interdépendants : les défis de la mise en place d'un système d'alerte précoce. M.A.Sc. thesis. École Polytechnique de Montréal, Québec, Canada.
- Department of Homeland Security [DHS]. (2009). National Infrastructure Protection Plan. Retrieved 11 April 2011 from http://www.dhs.gov/files/programs/editorial_0827.shtm.
- Flynn, P. (2010). *The Handling of the H1N1 Pandemic: More Transparency Needed*. Council of Europe. Consulted on May 17, 2011, retrieved from <http://assembly.coe.int>.
- Harvey, F., & Tulloch, D. (2006). Local-government data sharing: Evaluating the foundations of spatial data infrastructures. *International Journal of Geographical Information Science*, 20(1), 743–768.
- Ministère de la Sécurité Publique. (2010). *Démarche gouvernementale de résilience des systèmes essentiels*. Consulted on February 15, 2011, retrieved from <http://www.securitepublique.gouv.qc.ca/securite-civile/securite-civile-quebec/activites-evenements/colloque/colloque-2009/1173.html>.

- Public Safety and Emergency Preparedness Canada. (2006). *Ontario–U.S. Power Outage—Impacts on Critical Infrastructure*. http://www.publicsafety.gc.ca/prg/em/_fl/ont-us-power-e.pdf.
- Public Safety Canada. (2010). *Critical Infrastructure*. Consulted on May 17, 2011, retrieved from <http://www.publicsafety.gc.ca/prg/em/ci/index-eng.aspx>.
- Robert, B., De Calan, R., & Morabito, L. (2008). Modelling interdependencies among critical infrastructures. *International Journal of Critical Infrastructures*, 4(4), 392–408.
- Robert, B., & Morabito, L. (2009). *Réduire la vulnérabilité des infrastructures essentielles: guide méthodologique*. Paris: Tec&Doc.
- United Nations. (2006). *Global Survey on Early Warning Systems*.
- US DHS. (2002). *HSPD #3: Homeland Security Advisory System*. Consulted on October 8, 2010, retrieved from www.dhs.gov.
- US DHS. (2011a). *National Terrorism Advisory System*. Consulted on February 9, 2011, retrieved from www.dhs.gov.
- US DHS. (2011b). *Secretary Napolitano Announces New National Terrorism Advisory System to More Effectively Communicate Information about Terrorist Threats to the American Public*. Consulted on February 11, 2011, retrieved from http://www.dhs.gov/ynews/releases/pr_1296158119383.shtm.
- Vincent, C. (2010, January 28). L'OMS sommée de s'expliquer sur la grippe A. *Le Monde*. Retrieved from www.lemonde.fr.
- Voller, L., & Villesen, K. (2009, November 15). Stærk lobbyisme bag WHO-beslutning om massevaccination. *Information*. Retrieved from <http://www.information.dk/215355>.
- WHO. (2009). *Pandemic Influenza Preparedness and Response*. Consulted on February 11, 2011, retrieved from <http://www.who.int/csr/disease/influenza/en/index.html>.